EstEID

Turvakiibi rakenduse kasutusjuhend

Dokumendi versioon: 01.11.2003

Sisukord

1 Kellele on dokument suunatud

See dokument on mõeldud programmeerijaile, kes programmeerivad EstEID kaardiga vahetult suhtlevaid rakendusi või ohjureid, mis suhtlevad kaardiga kaardilugeja ohjuri, näiteks PC/SC, CT-API vms, kaudu. Dokumendis antakse üksikasjalik kirjeldus kaardi käsustiku kasutamise kohta.

Dokument ei ole vajalik neile, kes kirjutavad rakendusi, mis kasutavad EstEID kaarti olemasoleva kõrge taseme ohjuri (näit. Cryptoki või Microsoft CSP) kaudu.

Dokumendist arusaamine eeldab, et lugeja on tuttav kiipkaartidega suhtlemise üldiste põhimõtetega.

2 Kasutatud lühendid

MF	Juurkataloog turvakiibi failisüsteemis (ingl. k. Master File)
APDU	Kiibi rakendusprotokolli ühik
Kaardihalduskeskus	Institutsioon, kes teostab EstEID kaartide haldamise operatsioone kiibi haldaja volitusel
ICV	3DES algoritmi initsialisatsioonivektor
MAC	krüptograafiline kontrollsumma (ingl k. *Message Authentication Code*)
SK1, SK2	Sessioonivõtmed
SSC	sõnumiloendur *(ingl. k. Send Sequence Counter*)

3 Kaardi äratundmine

Kaardi äratundmiseks kasutatakse ATR stringi, mille kaart väljastab alglaadimisel. EstEID kaardil on kaks ATR stringi, nn. "külm ATR", mille kaart väljastab pärast pingestamist (st lugejasse sisestamist) ja nn "soe ATR", mille kaart väljastab pärast kaardilugeja algatatud alglaadimist.

EstEID kaardi "külm ATR" on järgmine[1]:

Bait nr.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
Väärtus	3B	FE	94	00	FF	80	B1	FA	45	1F	03	45	73	74	45	49	44

11	12	13	14	15	16	17	18	19
20	76	65	72	20	31	2E	30	43

[1] Siin ja edaspidi kasutatakse kuueteistkümnendsüsteemi numbreid, kui ei ole märgitud kümnendsüsteemi kasutamist märkega (dec).

EstEID kaardi "soe ATR" on järgmine:

Bait nr.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
Väärtus	3B	6E	00	FF	45	73	74	45	49	44	20	76	65	72	20	31	2E	30

ATR stringi baitide tähendused on defineeritud standardis ISO 7816-3. Baidid 0..A külmas ATR's ja baidid 0..3 soojas ATR's sisaldavad kaardi kommunikatsiooniprotokolli parameetreid. Rakendustele, mis suhtlevad kaardiga läbi olemasolevate ohjurite (n PC/SC, CT-API) ei oma need parameetrid tähendust, kuna nendega tegeleb ohjur.Tähtsad on baidid B..18 külmas ATR's ja 4..10 soojas ATR's. Need on nn. "ajaloolised baidid" *(ingl. "historical bytes "),* mille järgi rakendus teeb kindlaks, mis tüüpi kaardiga on tegemist. EstEID kaardil on need baidid järgmised:

EstEID∪ver∪1.0, kus

∪ on tühik

Märkus: ATR ajaloolised baidid ei ole standardiseeritud (ISO 7816-4 teeb küll katse neid baite standardiseerida, kuid praktikas ei ole see kasutust leidnud). Järelikult ei tähenda see, kui kiipkaart väljastab EstEID kaardi ATR 'ga sarnase ATR, et tegemist on EstEID kaardiga.. Veelgi enam, alati võib programmeerida mõne muu kiipkaardi nii, et see käitub sarnaselt EstEID kaardiga.. EstEID kaardi elektroonne atribuut on kaardil paiknevad salajased võtmed, mille avaliku poole on sertifitseerinud riiklik sertifitseerimiskeskus ning visuaalsed atribuudid on personaliseerimisel kaardile kantud turvaelemendid ja valdaja andmed. Küll võib aga väita, et kui kaardi ATR ei vasta EstEID kaardi ATR 'le, siis ei ole tegemist EstEID kaardiga.

4 T=0 või T=1?

Standard ISO 7816-3 ja selle lisa 1 näevad kiipkaartidega suhtlemiseks ette kaks protokolli - T=0 ja T=1, kusjuures protokollide erinevusega tuleb arvestada mitte ainult madala taseme ohjuri sees, vaid ka rakenduses, mis suhtleb kaardiga näiteks PC/SC tasemel.

EstEID kaart toetab mõlemat protokolli, kusjuures pärast alglaadimist lülitab kaart sisse T=0 protokolli. Kaarti kasutav rakendus võib vahetult pärast alglaadimist lülitada kaardi ümber T=1 protokollile. PC/SC käsustikus puuduvad mugavad võimalused sellise operatsiooni teostamiseks, küll aga suudavad seda mõnede lugejate PC/SC ohjurid, kui neilt on initsialiseerimisel nõutud kaardiga suhtlemist T=1 abil.

T=0 ja T=1 protokollide erinevusega tuleb kaarti kasutavas rakenduses arvestada selliste käskude puhul, kus käsk kaardile sisaldab andmeid ning ka kaardi vastus sisaldab andmeid. Niisugused käsud on failide lugemine kaardilt, SSL-kutsungile vastuse arvutamine, allkirja arvutamine ja sessioonivõtme dekrüptimine. Protokolli eripäraga mittearvestamine viib nende käskude juures veasituatsiooni.

Kuna T=0 protokollis saab EstEID kaardiga teostada kõiki operatsioone, siis puudub üldjuhul vajadus T=1 kasutamiseks, kuigi ka selle protokolli all on kõik operatsioonid teostatavad.

Samas tuleb T=0 jaoks programmeerides arvestada, et kaart võib saadetud käsule positiivse vastusena vastata koodiga "61 L". L (üks bait) näitab siin, kui mitu baiti andmeid on kaardil väljastamist ootamas. Nende baitide lugemiseks tuleb kaardile anda uus käsk:

CLA	INS	P1	P2	Le
00	C0	00	00	L

Näide: Kaart vastas käsule koodidega "61 0A", mis tähendab, et kaardil on ootamas 10 (dec) baiti. Nende baitide lugemiseks saadame:

CLA	INS	P1	P2	Le
00	C0	00	00	0A

Kaart vastab:

Väljastatavad baidid	OK trailer
00 00 00 00 00 00 00 00 00 00	90 00

5 PIN1, PIN2 ja PUK koodi muutmine

PIN1, PIN2 ja PUK koodi muutmine toimub järgmise käsuga:

CLA	INS	P1	P2	Lc	Senine PIN või PUK	Uus PIN või PUK
00	24	00	PIN-koodi number. PUK = 00 PIN1 = 01 PIN2 = 02	Senise PIN pikkus + uue PIN pikkus	ASCII koodidena	ASCII koodidena

Näide: Olgu senine PIN1 "1234" ja uus PIN1 "54321". Muudame PIN1-koodi järgmise käsuga:

CLA	INS	P1	P2	Lc	Senine PIN1	Uus PIN1
00	24	00	01	09	3132 33 34	35 34 33 32 31

Näide: Olgu senine PUK "12345678" ja uus PUK "1234567890". Muudame PUK-koodi järgmise käsuga:

CLA	INS	P1	P2	Lc	Senine PUK	Uus PUK
00	24	00	00	12	3132 33 34 35 36 37 38	31 32 33 34 35 36 37 38 39 30

6 PIN1 ja PIN2 koodide lahtiblokeerimine

PIN1, PIN2 ja PUK koodidel on EstEID kaardis valesisestuste loendurid *(ingl. retry counters),* mille algväärtus on 3. See tähendab, et pärast kolme järjestikust valesisestust koodid lukustuvad (igal koodil on eraldi loendur, ühe koodi valesti sisestamine ei muuda teiste koodide loendureid, st PIN1 valesti sisestamine ei muuda PIN2 ega PUK valesisestuste loendurit ega blokeeri neid).

Blokeerunud PIN1 ja PIN2 võib lahti blokeerida PUK-koodi abil. Blokeerunud PUK-koodi ei ole kaardi kasutajal võimalik lahti blokeerida. Blokeerunud PUK-koodiga kaardi taas kasutuskõlblikuks muutmiseks tuleb pöörduda vastava teenuse pakkuja poole.

PIN-koode võib EstEID kaardil lahti blokeerida kahte moodi:

1) jättes lahtiblokeeritava PIN-koodi samaks või
2) ühtlasi asendades lahtiblokeeritava PIN-koodi uuega.

PIN-koodi lahtiblokeerimine, jättes koodi samaks, toimub järgmiste käskudega: 1) Verifitseerime PUK- koodi:

CLA	INS	P1	P2	Lc	PUK
00	20	00	PUK-koodi number = 00	PUK-koodi pikkus	ASCII koodidena

2) Blokeerime PIN-koodi lahti:

CLA	INS	P1	P2
00	2C	03	PIN-koodi number, PIN1 = 01 PIN2 = 02

Näide: Olgu PUK "12345678" ja blokeerunud PIN1. Lahtiblokeerimiseks saadame: 1) Verifitseerime PUK- koodi:

CLA	INS	P1	P2	Lc	PUK
00	20	00	00	08	3132 33 34 35 36 37 38

2) Blokeerime PIN1 lahti:

CLA	INS	P1	P2
00	2C	03	01

PIN-koodi lahtiblokeerimine, asendades ühtlasi senise koodi uuega, toimub järgmise käsuga:

CLA	INS	P1	P2	Lc	PUK	Uus PIN
00	2C	00	PIN-koodi number, PIN1 = 01 PIN2 = 02	PUK-koodi pikkus + uue PIN pikkus	ASCII koodidena	ASCII koodidena

Näide: Olgu PUK "12345678" ja blokeerunud PIN1, millele pärast lahtiblokeerimist soovime anda väärtuse "1234". Lahtiblokeerimiseks saadame:

CLA	INS	P1	P2	Lc	PUK	Uus PIN1
00	2C	00	01	0C	31 32 33 34 35 36 37 38	31 32 33 34

Märkus: Kui PIN-kood ei ole blokeerunud (st seda ei ole kolm korda järjest valesti sisestatud), siis vastab EstEID kaart lahtiblokeerimise käsule veateatega.

7 Andmete lugemine isikuandmete failist

EstEID kaardil on isikuandmete fail, mille FID *(ingl. File Identifier)* on 'PD' ehk '50 44'. See on muutuva kirjepikkusega fail *(ingl. variable-length recordfile),* mis sisaldab kaardile personaliseerimisel kantud infot elektroonsel kujul (va foto ja allkirja kujutis) ja on hetkel defineeritud järgnevalt:

Kirje number	Sisu	Maksimaalne pikkus (baiti,
1	Perenimi	28
2	Eesnimede rida 1	15
3	Eesnimede rida 2	15
4	Sugu	1
5	Kodakondsus (3 tähte, alati EST)	3
6	Sünnikuupäev (pp.kk.aaaa)	10
7	Isikukood	11
8	Dokumendi number	8
9	Kehtivuse viimane päev (pp.kk.aaaa)	10
10	Sünnikoht	35
11	Väljaandmise kuupäev (pp.kk.aaaa)	10
12	Elamisloa tüüp	50
13	Märkuste rida 1	50

14	Märkuste rida 2	50
15	Märkuste rida 3	50
16	Märkuste rida 4	50

Hetkel sisaldab fail 16 kirjet ning kirje maksimaalne pikkus on 50 (dec) baiti.

On olemas tehnilised võimalused, et personaliseerimisprotsessi käigus täiendatakse faili uute kirjete lisamisega faili lõppu. Samuti võidakse muuta kirje maksimaalset pikkust.

Andmete lugemiseks failist toimime järgnevalt:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Valime faili 5044 käsuga SELECT FILE. Käsu anname sellisel kujul, et EstEID kaart annab vastuseks faili päise:

T=0 korral saadame:

CLA	INS	P1	P2	Lc	FID
00	A4	02	04	02	50 44

T=1 korral saadame:

CLA	INS	P1	P2	Lc	FID	Le
00	A4	02	04	02	50 44	00

Faili päise pikkus ei ole üldjuhul eelnevalt teada. Seetõttu anname Le baidi ette väärtusega 0.

Kaart vastab:

Bait nr.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	..
Väärtus	62	17	82	05	04	41	00	32	10	83	02	50	44	85	02	01	00	

11	12	13	14	15	16	17	18
8A	01	05	A1	03	8B	01	01

Kirje maksimaalne pikkus on baidis nr 7 ja kirjete arv baidis nr 8 (nb! kuueteistkümnendväärtused).

Märkus: EstEID kaart hoiab informatsiooni failipäistes TLV (Tag Length Value) objektide kujul. Kirje maksimaalne pikkus on konteinerobjektis (ingl. compound data object) 62 sisalduva objekti 82 baidis 3 (loendus algab ühest) ja kirjete arv baidis 4. Korrektne oleks kirje maksimaalse pikkuse ja kirjete arvu leidmiseks parsida failipäise sisu. Kuna agafailipäis EstEID kaardis (tõenäoliselt) ei muutu, annab lihtsalt 7.ja 8. baidi lugemine ka (tõenäoliselt) õige tulemuse.

4) Loeme kirje 1 sellest failist:

CLA	INS	P1 (kirje number)	P2	Le
00	B2	01	04	00

Kui kasutusel on protokoll T=0, siis võib Le ka ära jätta. Le on jällegi 0, kuna kirje pikkus ei ole eelnevalt teada.

Kasutades protokolli T=0 vastab kaart:

Kaardis on baite ootel	Ootel baitide arv (perenime pikkus)
61	...

Loeme kaardilt perenime:

CLA	INS	P1	P2	Le
00	C0	00	00	Perenime pikkus

Kaart vastab (kasutades T=1 protokolli, saame sellise vastuse kohe):

Perenimi	OK Trailer
…	90 00

Teised kirjed loetakse analoogselt.

8 Loendurite lugemine kaardilt

EstEID kaardil on järgmised loendurid:

1) PIN1 valesisestuste loendur
2) PIN2 valesisestuste loendur
3) PUK valesisestuste loendur
4) Paroollause 1[2] valesisestuste loendur

[2] Paroollaused *(ingl. passphase)* on EstEID kaardil kasutaja autentimiseks kasutatavad objektid, mida saab kasutada sarnaselt PIN1 ja PIN2'ga. Nende kasutamist vaadeldakse juhendi

5) Paroollause 2 valesisestuste loendur
6) Signeerimisvõtme versiooni 1[3] kasutuskordade loendur
7) Signeerimisvõtme versiooni 2 kasutuskordade loendur
8) Autentimisvõtme versiooni 1 kasutuskordade loendur
9) Autentimisvõtme versiooni 2 kasutuskordade loendur

PIN- ja PUK-koodide valesisestuste loendurid on kaardi juurkataloogi failis, mille FID (File Identifikator) on 0016. PIN1 kohta käib selle faili kirje 1, PIN2 kohta kirje 2 ja PUK kohta kirje 3. Valesisestuste loendurite väärtuste leidmiseks toimime nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime faili 0016 käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	02	0C	02	00 16

3) Loeme kirje 1 sellest failist:

CLA	INS	P1 (kirje number)	P2	Le
00	B2	01	04	00

Kuna fail 0016 on muutuva kirjepikkusega struktureeritud fail *(ingl. variable record lengthfile),* siis ei ole võimalik ette teada kaardilt loetavate baitide hulka. Seetõttu anname Le baidi ette väärtusega 0. Kasutades protokolli T=0 võib Le ka ära jätta, T=1 korral peab Le bait olema.

Kaardilt loetakse kirje:

Bait nr.	0	1	2	3	4	5	6	7	8	9
Väärtus	80	01	03	90	01	03	83	02	00	00

PIN1 valekasutuste loendur on baidis nr 5.

NB! Valekasutuste loenduri algväärtus on 3 ning blokeerunud kaardil on selle väärtus 0, seega näitab loendur, mitu PIN sisestuskatset on veel järel.

Märkus: EstEID kaart hoiab informatsiooni failikirjetes TLV (Tag Length Value)

järgnevas osas

[3] EstEID kaart võimaldab (pärast teatud autentimisoperatsioone) genereerida uued võtmepaarid. Eelmised võtmepaarid säilitatakse. Uute võtmepaaride genereerimist vaadeldakse allpool. Pärast personaliseerimist (ja kuni uute võtmepaaride genereerimiseni) on kasutusel võtmete versioon 1

objektide kujul. PIN valesisestuste loendur on objektis tagiga 90 ja pikkusega 01. Korrektne oleks lugeda loenduri väärtus, parsides kirje sisu. Kuna aga kirje kuju kaardi kasutusaja jooksul(tõenäoliselt) ei muutu, annab lihtsalt 5. baidi lugemine ka (tõenäoliselt) õige tulemuse.

4) Analoogse käsuga loeme kirje 2, milles sisaldub PIN2 valesisestuste loendur:

CLA	INS	P1 (kirje number)	P2	Le
00	B2	02	04	00

5) PUK valesisestuste loenduri teadasaamiseks loeme kirje 3:

CLA	INS	P1 (kirje number)	P2	Le
00	B2	03	04	00

Loetud kirje on järgmine:

Bait nr.	0	1	2	3	4	5
Väärtus	80	01	03	90	01	03

Valesisestuste loendur on jällegi baidis nr 5.

Paroollausete valesisestuste loendurid on juurkataloogi failis 0013 kirjetes 5 (paroollause 1) ja 6 (paroollause 2).

Paroollause 5 valesisestuste loenduri lugemiseks toimime nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime faili 0013 käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	02	0C	02	00 13

3) Loeme kirje 5 sellest failist:

CLA	INS	P1 (kirje number)	P2	Le
00	B2	05	04	00

Fail 0013 on samuti muutuva kirjepikkusega struktureeritud fail. Kasutades protokolli T=0 võib Le ka ära jätta, T=1 korral peab Le bait olema.

Kaardilt loetakse kirje:

Bait nr.	0	1	2	3	4	5	6	7	8	9	A	... kirje kogupikkus on 28(hex) baiti
Väärtus	83	02	04	00	C1	02	81	10	90	01	FF	...

Paroollause valekasutuste loendur on baidis nr A. Selle algväärtus on FF ning igal paroollause 1 valesisestusel väheneb loendur ühe võrra. Kui loendur on jõudnud nulli, ei ole paroollause enam kasutatav ning kaardi kasutamisel tuleb autentida PIN-koodidega või kaart vahetada. Paroollause valekasutuste loendur ei uuene paroollause õigel sisestamisel.

Paroollause 2 loendur on analoogselt kirjes nr 6.

Salajaste võtmete kasutuskordade loendurid on kataloogis EEEE failis 0013 järgmistes kirjetes:

Võtmeversioon	**Faili EF/EEEE/0013 kirje number**
Signeerimisvõtme versioon 1	1
Signeerimisvõtme versioon 2	2
Autentimisvõtme versioon 1	3
Autentimisvõtme versioon 2	4

Selleks, et teada saada, mitu korda on kasutatud signeerimisvõtme versiooni 1, toimime järgmiselt:

5) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

6) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

7) Valime faili 0013 käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	02	0C	02	00 13

8)	INS	P1 (kirje number)	P2	Le
00	B2	01	04	00

Fail 0013 on selles kataloogis fikseeritud kirjepikkusega struktureeritud fail (kirje pikkus on 4F), kuid kehtima jääb sama reegel: kasutades protokolli T=0, võib Le ka ära jätta, T=1 korral peab Le bait olema.

Kaardilt loetakse kirje:

Bait nr.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	...
Väärtus	83	04	01	00	10	01	C0	02	81	80	91	03	FF	FF	FF	

Võtme kasutuskordade loendur on kolmebaidilise väärtusena baitides nr C..E, kusjuures vanem bait on vasakul. Seega saadakse loenduri väärtus järgmiselt:

<Bait C väärtus>*10^2 + <Bait D väärtus>*10 + <Bait E väärtus>

Võtme kasutuskordade loenduri algväärtus on FFFFFF ning võtme igal kasutusel lahutatakse sellest 1. Selleks, et saada teada, mitu korda on võtit kasutatud, tuleb kaardilt loetud väärtus lahutada FFFFFF'st.

Teiste võtmete kasutuskordade arv loetakse kaardilt analoogselt.

9 Sertifikaatide lugemine kaardilt

Sertifikaadid on EstEID kaardil kataloogis EEEE jadafailide *(ingl. transparent fil*e) kujul. Kuna planeeritud on sertifikaatide uuendamine kaardi kastusaja jooksul, reserveeritakse personaliseerimise käigus sertifikaatide jaoks fikseeritud suurusega failid, et garanteerida uute (ja võimalik, et mahult suuremate) sertifikaatide kaardile kirjutamise võimalikkus.
Ülejäänud osa failist täidetakse järgneva skeemi järgi:

Sertifikaat	Bait 80	00 .. 00

st sertifikaadi lõppu lisatakse bait 80 ning ülejäänud osa faili lõpuni täidetakse nullbaitidega.

Sertifikaadid on järgmistes failides:

Sertifikaat	FID	Maht (hex baiti)
Digitaalset isikutuvastamist võimaldav sertifikaat	EF/EEEE/AACE	600
Digitaalset allkirjastamist võimaldav sertifikaat	EF/EEEE/DDCE	600

Failide mahud võivad muutuda. Allpool on näidatud, kuidas teha kindlaks kaardil asuva faili tegelik suurus.

Digitaalset isikutuvastust võimaldava sertifikaadi (analoogselt ka teiste sertifikaatide) lugemiseks kaardilt toimime nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Valime faili AACE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	02	0C	02	AACE

Kaart vastab:

Bait nr.	0	1	2	3	4	5	6	7	8	9	A	B	C	... vastuse kogupikkus on 1A baiti
Väärtus	62	18	82	01	01	83	02	AA	CE	85	02	06	00	...

Faili maht on vastuse baitides B ja C, antud

juhul 600 (hex).

4) Loeme faili sisu käsuga READ BINARY:

CLA	INS	P1(offsetMSB)	P2(offsetLSB)	Le (number of bytes to read)
00	B0	00	00	64

See käsk loeb 64 (hex) baiti faili algusest. Le on siin vajalik nii T=0 kui T=1 korral, sest ta näitab, mitu baiti tuleb lugeda. P1 ja P2 näitavad aadressi failis, millelt lugeda. Näiteks lugemiseks aadressilt 120 (hex) P1=01 ja P2=20. Le maksimumväärtus on FE.

10 SSL kutsungile vastuse arvutamine

SSL kutsungile *(ingl. SSL challenge)* vastuse arvutamine on PKCS#1 ver. 1.5 block type 1 järgi formateeritud kutsungi dekrüptimine RSA salajase võtmega. Vastuse arvutamiseks EstEID kaardis tuleb toimida nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EE EE

3) Seame kaardisisese turvakeskkonna *(ingl. security environment)* nr 1:

CLA	INS	P1	P2

00	22	F3	01

4) Verifitseerime PIN1:

CLA	INS	P1	P2	Lc	PIN1
00	20	00	PIN1-koodi number = 01	PIN1-koodi pikkus	ASCII koodidena

5) Saadame kaardile käsu kutsungi vastuse

arvutamiseks: a) T=0 korral saadame:

CLA	INS	P1	P2	Lc (kutsungi pikkus)	Kutsung
00	88	00	00	24	....

b) T= 1 korral saadame

CLA	INS	P1	P2	Lc (kutsungi pikkus)	Kutsung	Le
00	88	00	00	24	....	80

EstEID kaart väljastab 80 (hex) baiti, mis on PKCS#1 ver. 1.5 block type 1 järgi formateeritud ja seejärel autentimisvõtmega krüptitud kutsung.

SSL standardi järgi on kutsungi pikkus 24 (hex) baiti, kuid EstEID kaart võimaldab arvutada vastuseid ka teistsuguste pikkustega kutsungitele.

11 Elektronallkirja arvutamine

Elektroonse allkirja arvutamine on PKCS#1 ver. 1.5 block type 1 järgi formateeritud räsiobjekti dekrüptimine RSA salajase võtmega.

EstEID kaart võimaldab arvutada elektroonset allkirja kahel viisil:

a) andes ette allkirjastatava teksti räsi sisaldava objekti või
b) saates kaardile blokkide kaupa allkirjastatava teksti ning lastes kaardil selle
räsida.

Räsimisega kaardil võib allkirja arvutada siis, kui operatsioon toimub piiratud ressursiga seadmes, milles pole räsimise funktsiooni, näiteks POS-terminalis.

11.1 Elektronallkirja arvutamine, kui räsi on valmis

Selleks tuleb toimida nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Seame kaardisisese turvakeskkonna *(ingl. security environment)* nr 1:

CLA	INS	P1	P2
00	22	F3	01

4) Verifitseerime PIN2:

CLA	INS	P1	P2	Lc	PIN2
00	20	00	PIN2-koodi number = 02	PIN2-koodi pikkus	ASCII koodidena

5) Saadame kaardile käsu allkirja arvutamiseks:

a) T=0 korral saadame:

CLA	INS	P1	P2	Lc (räsiobjekti pikkus)	Räsiobjekt
00	2A	9E	9A	23	....

b) T=1 korral saadame:

CLA	INS	P1	P2	Lc (räsiobjekti pikkus)	Räsiobjekt	Le
00	2A	9E	9A	23	....	80

EstEID kaart väljastab 80 (hex) baiti, mis on PKCS#1 ver. 1.5 block type 1 järgi formateeritud ja seejärel autentimisvõtmega krüptitud räsiobjekt.

Näide: Olgu allkirjastatava teksti SHA-1 räsi 0102030405060708090A0B0C0D0E0F1012131415 (hex), PIN2 "12345" ja kasutusel protokoll T=0. Arvutame elektroonse allkirja:

1) Valime juurkataloogi:

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Seame kaardisisese turvakeskkonna nr. 1:

CLA	INS	P1	P2
00	22	F3	01

4) Verifitseerime PIN2:

CLA	INS	P1	P2	Lc	PIN2
00	20	00	02	05	31 32 33 34 35

5) Saadame kaardile käsu allkirja arvutamiseks:

CLA	INS	P1	P2	Lc	Räsiobjekt
00	2A	9E	9A	23	30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 12 13 14 15

Kaart vastab:

Kaardis on baite ootel	Ootel baitide arv
61	80

6) Loeme ootel baidid:

CLA	INS	P1	P2	Le
00	C0	00	00	80

Kaart vastab:

Elektroonne allkiri: 80 (hex) baiti	OK trailer
—	90 00

11.2 Elektronallkirja arvutamine räsimisega kaardis

Elektronallkirja arvutamisel räsimisega kaardis on esimesed neli operatsiooni samad:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Seame kaardisisese turvakeskkonna *(ingl. security environment)* nr. 1:

CLA	INS	P1	P2
00	22	F3	01

4) Verifitseerime PIN2:

CLA	INS	P1	P2	Lc	PIN2
00	20	00	PIN2-koodi number = 02	PIN2-koodi pikkus	ASCII koodidena

5) Räsime allkirjastatava teksti kaardis.

Räsimiseks tuleb tekst saata kaardile 40 (hex)-baidiste blokkidena, kusjuures viimane blokk võib olla lühem.

Blokid, viimane välja arvatud, on niisugusel kujul:

CLA	INS	P1	P2	Lc	Andmed: 80 40 <40(hex)-baidine andmeblokk>
10	2A	90	A0	42	80 40….

Viimane blokk on kujul:

CLA	INS	P1	P2	Lc	Andmed: 80 <viimase bloki pikkus><viimane andmeblokk>
00	2A	90	A0	Viimase bloki pikkus + 2	80L….

Viimase bloki pikkus võib olla ka 40(hex)

baiti. Kui kasutusel on protokoll T=0, siis

vastab kaart

Kaardis on baite ootel	Ootel baitide arv - SHA-1 räsi pikkus
61	14

ning kaardil arvutatud räsi võib välja lugeda käsuga

CLA	INS	P1	P2	Le
00	C0	00	00	14

Kui kasutusel on protokoll T=1, võib viimast blokki kaardile saatva käsu lõppu lisada Le=14, mispeale kaart saadab tagasi arvutatud räsi. Kui Le käsu lõppu lisatud ei ole, vastab kaart T=1 protokolli all lihtsalt 90 00.

6) Saadame kaardile käsu arvutada allkiri kaardil oleva räsi kohta. Kaart lisab ise 20(dec) baidise räsi ette ASN.1 SHA-1 räsiobjekti moodustamiseks vajalikud baidid.

a) T=0 korral saadame:

CLA	INS	P1	P2
00	2A	9E	9A

b) T=1 korral saadame:

CLA	INS	P1	P2	Le
00	2A	9E	9A	80

Näide: Olgu vaja arvutada allkiri järgmisele tekstile (teksti pikkus on 8A baiti, ∪ tähistab tühikut), olgu PIN2="12345" ja kasutusel olgu protokoll T=0.

AutoUonUsõitjateUvõiUveosteUveoksUvõiUsõidukiteU haakesUvedamiseksUvõiUeritöödeUtegemiseksUettenähtudUvähe maltUneljarattalineUmootorsõiduk.

1) Valime juurkataloogi:

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Seame kaardisisese turvakeskkonna nr 1:

CLA	INS	P1	P2
00	22	F3	01

4) Verifitseerime PIN2:

CLA	INS	P1	P2	Lc	PIN2
00	20	00	02	05	31 32 33 34 35

5) Kuna teksti pikkus on 8A baiti, tuleb räsi arvutada kolmes blokis, millest kahe esimese pikkus on 40(hex) baiti ja viimase pikkus on A.

Blokk1:

CLA	INS	P1	P2	Lc	80 40 <esimene 40(hex)-baidine andmeblokk>
10	2A	90	A0	42	80 40 AutoUonUsõitjateUvõiUveosteUveoksUvõiUsõidukiteU haakesUvedamisek

Blokk 2:

CLA	INS	P1	P2	Lc	80 40 <teine 40(hex)-baidine andmeblokk>

10	2A	90	A0	42	80 40 s∪või∪eritöödе∪tegemiseks∪ettenähtud∪v ähemalt∪neljarattaline∪mootorsõiduk

Blokk 3:

CLA	INS	P1	P2	Lc	80 L <viimane 40(hex)- baidine või lühem andmeblokk>
00	2A	90	A0	0C	80 0A torsõiduk.

Kaart vastab:

Kaardis on baite ootel	Ootel baitide arv
61	14

7) Loeme kaardilt arvutatud räsi (selle operatsiooni võib ka ära jätta):

CLA	INS	P1	P2	Le
00	C0	00	00	14

8) Arvutame elektroonse allkirja:

CLA	INS	P1	P2
00	2A	9E	9A

Kaart vastab:

Kaardis on baite ootel	Ootel baitide arv
61	80

9) Loeme kaardilt elektroonse allkirja:

CLA	INS	P1	P2	Le
00	C0	00	00	80

Kaart vastab:

80 (hex baiti)	OK trailer
……	90 00

12 Sessioonivõtme dekrüptimine

Sessioonivõtme dekrüptimisel dekrüptitakse salajase võtmega RSA krüptoblokk, mis on saadud PKCS#1 ver. 1.5 block type 2 järgi formateeritud andmebloki

krüptimisel vastava avaliku võtmega. Ühtlasi parsib EstEID kaart dekrüptimise tulemusel saadud andmebloki ning saadab välja vaid selles sisaldunud andmed.

Seega, NB!: Kui dekrüptimiseks etteantud andmeblokk ei ole vastava avaliku võtmega

krüptitud PKCS#1 ver. 1.5 block type 2 järgi krüptitud andmeblokk, siis tekib EstEID kaardis veasituatsioon.

Dekrüptimise operatsioon on võimalik nii autentimis- kui signeerimisvõtmega.

Sessioonivõtme dekrüptimiseks tuleb toimida nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Seame kaardisisese turvakeskkonna *(ingl. security environment)* nr. 6:

CLA	INS	P1	P2
00	22	F3	06

4) Modifitseerime kaardisisest turvakeskkonda, kustutades viida autentimisvõtmele, st. ütleme kaardile, et autentimise operatsioone ei ole järgnevalt vaja teha[4]:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	A4	02	83 00

5) Modifitseerime kaardisisest turvakeskkonda, kustutades viida signeerimisvõtmele, st ütleme kaardile, et signeerimise operatsioone ei ole järgnevalt vaja teha:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	B6	02	83 00

6) Modifitseerime kaardisisest turvakeskkonda, seades viida võtmele, millega soovime dekrüptimise operatsiooni sooritada.

[4] Nende operatsioonide olemuse kohta võib lähemat infot saada MICARDO User Manual'st

Kui soovime dekrüptida autentimisvõtmega, saadame järgneva käsu[5]:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	B8	05	83 03 80 11 00

Kui soovime dekrüptida signeerimisvõtmega, saadame järgneva käsu:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	B8	05	83 03 80 01 00

7) Kui soovime dekrüptida autentimisvõtmega, verifitseerime PIN1-koodi:

CLA	INS	P1	P2	Lc	PIN1
00	20	00	PIN1-koodi number = 01	PIN1-koodi pikkus	ASCII koodidena

Kui soovime dekrüptida signeerimisvõtmega, verifitseerime PIN2-koodi:

CLA	INS	P1	P2	Lc	PIN2
00	20	00	PIN2-koodi number = 02	PIN2-koodi pikkus	ASCII koodidena

8) Saadame kaardile käsu bloki dekrüptimiseks. Krüptitud bloki pikkus on 80(hex) baiti, kuna kasutatavad võtmed on 1024 bitti pikad:

a) T=0 korral saadame:

CLA	INS	P1	P2	Lc (1+80 baiti)	1 bait väärtusega 00	Krüptitud blokk
00	2A	80	86	81	00	

b) T=1 korral saadame:

CLA	INS	P1	P2	Lc (1+80 baiti)	1bait väärtusega 00	Krüptitud blokk	Le
00	2A	80	86	81	00	....	00

Le anname jällegi ette 00, kuna krüptoblokis oleva dekrüptitud andmebloki pikkus ei ole teada.

EstEID kaart vastab krüptoblokis sisaldunud andmeblokiga.

Näide: Olgu vaja dekrüptida blokk signeerimisvõtmega, olgu PIN2="12345" ja kasutusel protokoll T=0.

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE. Pärast

[5] Sellisel kujul on see käsk siis, kui kaardil ei ole pärast personaliseerimist genereeritud uut võtmepaari. Kui sellist eeldust ei ole võimalik kasutada, siis tuleb teostada veel mõned lisaoperatsioonid. Seda kirjeldatakse täpsemalt allpool

kaardi alglaadimist võib selle käsu ka ära jätta, sest juurkataloog on siis vaikimisi valitud.

CLA	INS	P1	P2
00	A4	00	0C

2) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

3) Seame kaardisisese turvakeskkonna nr 6:

CLA	INS	P1	P2
00	22	F3	06

4) Modifitseerime kaardisisest turvakeskkonda, saates järgnevad kolm käsku:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	A4	02	83 00

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	B6	02	83 00

Seame signeerimisvõtme dekrüptimise operatsiooni teostamiseks, st ütleme kaardile, et järgnevad dekrüptimisoperatsioonid tuleb teostada signeerimisvõtmega. Selleks saadame:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	B8	05	83 03 80 01 00

5) Verifitseerime PIN2-koodi:

CLA	INS	P1	P2	Lc	PIN2
00	20	00	02	05	3132 33 34 35

6) Saada kaardile käsu bloki dekrüptimiseks:
me

CLA	INS	P1	P2	Lc (1+80 baiti)	1 bait väärtusega 00	Krüptitud blokk
00	2A	80	86	81	00	

Kaart vastab:

Kaardis on baite ootel	Ootel baitide arv (krüptoblokis sisaldunud andmete hulk baitides)
61	...

7) Loeme kaardilt elektroonse allkirja:

CLA	INS	P1	P2	Le (ootel baitide arv)
00	C0	00	00	...

Kaart vastab:

Krüptoblokis sisaldunud andmed	OK Trailer
….	90 00

13 Sertifikaatide uuendamine

EstEID kaardil on uuendatavad nii kasutajasertifikaadid (autentimissertifikaat ja signeerimissertifikaat) kui juursertifikaat (juhul, kui see on kaardile kirjutatud). Turvakaalutlustel ei ole lubatud sertifikaatide ülekirjutamine "otse" - ülekirjutamine on kaitstud turvamehhanismidega, mis ühtlasi tagavad ka, et sertifikaate on võimalik laadida vaid sellesse EstEID kaarti, millesse need kuuluvad. Katse laadida sertifikaat mõnesse teise EstEID kaarti, viib veasituatsiooni.

Rakendatav turvamehhanism seisneb selles, et kaardihalduskeskus ehk TMC *(ingl. Token Mangement Centre)* konverteerib sertifikaadi koodi käskudesse, mis sisaldavad vastavat MAC-koodi. Niisugusel kujul võtab see EstEID kaart, millesse sertifikaat kuulub selle ka vastu.

Sertifikaadi laadimise protseduur seisneb järgnevates operatsioonides:

1. Valida kaardil MF.
2. Seada kaardisisene turvakeskkond nr. 3.
3. Valida kaardil kataloog EE EE.
4. Verifitseerida PIN1-kood. PIN1-koodi verifitseerimine on mõeldud selleks,
   et garanteerida sertifikaadi uuendamine kaardil vaid kaardi kasutaja teadmisel.
5. Lugeda järjest käsud TMC poolt antud sertifikaadi laadimiskoodi failist ning saata need kaardile.

Sertifikaadi laadimiskoodi failides on käsud HEX (ehk BCD) vormingus, igal real üks käsk (ridade eraldaja on LF - 0x0A).

Sertifikaadi uuendamise protseduur käskude tasemel näeb välja nii:

1) Valime juurkataloogi (MF - *ingl. Master File)* käsuga SELECT FILE.

CLA	INS	P1	P2
00	A4	00	0C

2) Seame kaardisisese turvakeskkonna *(ingl. security environment)* nr 3:

CLA	INS	P1	P2
00	22	F3	03

3) Valime kataloogi EEEE käsuga SELECT FILE:

CLA	INS	P1	P2	Lc	FID
00	A4	01	0C	02	EEEE

4) Seame kataloogis EE EE uuesti kaardisisese turvakeskkonna *(ingl. security environment)* nr 3:

CLA	INS	P1	P2
00	22	F3	03

5) Verifitseerime PIN1-koodi:

CLA	INS	P1	P2	Lc	PIN1
00	20	00	PIN1-koodi number = 01	PIN1-koodi pikkus	ASCII koodidena

6) Laeme uue sertifikaadi kaardile järgmise algoritmi järgi:

```
While (! EndOfFile)
{
        Line = ReadLineFromFile;
        Convert Line from BCD to Binary;
        If Protocol == T0 Remove Le byte;
        Transmit Line to EstEID card;
        }
```

Kui kõik sertifikaadi laadimiskoodi failis sisaldunud käsud on saadetud kaardile, ongi sertifikaat uuendatud.

14. Paroollausete seadmine ja muutmine, operatsioonide teostamine, tuvastades kasutaja paroollausega

14.1. Paroollause kasutamise põhimõte

Paroollause on piiramatu pikkusega märkide jada, mida kasutatakse 3DES võtme tuletamiseks. Sama 3DES võti on salvestatud EstEID kaardile. Seda võtit on võimalik kasutada turvalise ühenduse loomiseks EstEID kaardi ja host-rakenduse vahel, kuid ka kasutaja tuvastamiseks, sest paroollauset, nagu PIN-koodigi, teab ainult kaardi õiguspärane kasutaja. Seega suudab ainult tema sisestada host-rakendusse (paroollause kaudu) salajase võtme, mille abil saab sooritada EstEID PKI operatsioone.

Paroollausega tuvastamise korral on operatsiooni sooritamise protseduuri sammude järjekord järgmine:

1. Kasutaja sisestab paroollause;
2. Host-rakendus tuletab paroollausest 3DES võtme;

3. Vastastikuse interaktsiooni käigus tuletavad kaart ja host-rakendus unikaalse sessioonivõtme;
4. Sessioonivõtmega krüptitakse kaardile saadetavate käskude sisu ning arvutatakse krüptograafilised kontrollsummad. Katse sooritada operatsiooni ebaõige võtmega viib veasituatsiooni. EstEID kaardilt saabuvad vastused on samuti krüptitud ning sisaldavad krüptograafilisi kontrollsummasid.

Allpool vaatleme näite varal iga sammu üksikasjalikult.

EstEID kaardil on kaks paroollausest tuletatavat võtit – 3DESKey1 ja 3DESKey2, millest esimene võimaldab sooritada operatsioone autentimisvõtmega ja teine allkirjastamisvõtmega. Katse sooritada operatsiooni teise 3DES võtmega (näiteks - arvutada elektroonilist allkirja 3DESKey1 abil), viib veasituatsiooni.

14.2. Võtme tuletamine paroollausest

Paroollausest võtme tuletamise protseduur on kokkuleppeline, mitte EstEID kaardi omadus. Vajadus ühtse protseduuri järele on tingitud sellest, et tagada sama paroollause kehtivus erinevates rakendustes.

Välja on pakutud järgmine protseduur:
arvutatakse paroollause SHA-1 räsi;
võetakse saadud räsi 16 vasakpoolsemat baiti;
iga baidi noorim bitt seatakse nii, et bait oleks paaritu, sest EstEID kaart nõuab seda. Vale paarsusega baidi sisaldumine EstEID kaardi võtmes viib veasituatsiooni.

Märkus: Valmistamise ajal seatakse EstEID kaardi mõlema 3DESKey väärtuseks 00..00 (kõik nullbaidid). Seda võtit ei sa kasutada, kuna nullbaidid on paarisbaidid.

Olgu paroollause1 (3DESKey1 tuletamiseks) järgmine:

Kaks∪kurja∪kukke∪kaklevad∪kuudi∪katusel.

ja paroollause2 (3DESKey2 tuletamiseks) järgmine (ka edaspidistes näidetes kasutatakse neid lauseid):

See∪on∪minu∪paroollause2.

kus ∪ tähistab tühikut.

Arvutame nende lausete SHA-1 räsid:

Paroollause1 räsi:

63	F0	EA	AD	E2	7E	5F	CA	D2	5A	09	CB	3F	E3	96	5E	43	7B	DA	F9

Paroollause2 räsi:

30	A1	DB	94	DF	29	BC	65	A8	17	25	2B	A6	73	88	FE	9B	7B	D6	43

Võtame räsidest 16 vasakpoolsemat baiti ning seame iga baidi noorema biti nii, et bait oleks paaritu. Tulemuseks saame:

3DESKey1:

62	**F1**	EA	AD	**E3**	**7F**	**5E**	**CB**	**D3**	**5B**	**08**	CB	**3E**	E3	**97**	5E

3DESKey2:

31	A1	**DA**	94	DF	29	BC	**64**	A8	**16**	25	**2A**	**A7**	73	**89**	FE

Neid võtmeid kasutatakse ka edaspidistes näidetes.

14.3. Paroollausete seadmine kaardile

3DESKey1 asub juurkataloogi (MF) failis FID=0010 kirjes nr 1 ja 3DESKey2 asub sama faili kirjes nr 2.

3DESKey seadmine seisneb võtme väärtuse kirjutamisel vastavasse kirjesse järgmise nüansiga:

3DESKey1 võtme väärtuse ette tuleb lisada baidid ’04 00’ ja 3DESKey2 väärtuse ette tuleb lisada baidid ’05 00’[6]. Seega on kummagi võtmekirje pikkuseks 0x12 baiti.

14.3.1. Paroollause seadmine PIN2-koodiga autoriseerides

Paroollause1 seadmiseks autoriseerimisel PIN2-koodiga toimime järgmiselt:

1. Seame kaardisisese turvakeskkonna nr 1:

CLA	INS	P1	P2
00	22	F3	01

2. Verifitseerime PIN2-koodi:

CLA	INS	P1	P2	Lc	PIN2				
00	20	00	02	05	31	32	33	34	35

3. Valime juurkataloogi ja seejärel faili FID=0010

CLA	INS	P1	P2
00	A4	00	0C

CLA	INS	P1	P2	Lc	FID	
00	A4	02	0C	02	00	10

4. Kirjutame selle faili kirje nr 1 üle järgmise käsuga (P1 = kirje number):

CLA	INS	P1	P2	Lc	Võtme ID		Võtme väärtus														
00	DC	01	04	12	04	00	62	F1	EA	AD	E3	7F	5E	CB	D3	5B	08	CB	3E	E3	97	5E

Paroollause2 seadmiseks kirjutame võtme väärtuse sama faili kirjesse nr 2:

[6] Need on võtmete (järjekorra)numbrid EstEID kaardi sisemise struktuuri tarvis. Lähemalt vaata MICARDO kaardi juhendist.

CLA	INS	P1	P2	Lc	Võtme ID		Võtme väärtus														
00	DC	02	04	12	05	00	31	A1	DA	94	DF	29	BC	64	A8	16	25	2A	A7	73	89	FE

14.3.2. Paroollause seadmine senise paroollausega autoriseerides

Paroollauset on võimalik seada (st kirjutada kaardile juurkataloogi faili FID=0010 võtme uus väärtus) ka autoriseerides senise (st momendil juurkataloogi failis FID=0010 oleva) võtmega.

Tuleb tunnistada, et see operatsioon on keerulisem, kui paroollause seadmine PIN2-ga autoriseerimisega, kuna eeldab EstEID turvalise kommunikatsiooni ülesseadmist kaardi ja host-rakenduse vahel.

NB! Kui PIN2-ga autoriseerides saame seada nii paroollause1 kui parollause2, siis senise paroollausega autoriseerides tuleb autoriseerida senise paroollausega1 uue parollause1 seadmiseks ja senise parollausega2 uue paroollause2 seadmiseks.

Olgu kehtivad paroollaused eelmises peatükis seatud paroollause1 = “Kaks kurja kukke kaklevad kuudi katusel.” ja paroollause2 = “See on minu paroollause2.”.

Olgu uus paroollause1 järgmine:

Kured∪läinud∪-∪kurjad∪ilmad.

kus ∪ tähistab tühikut.

Sellest paroollausest tuletatud võti 3DESKey1 on järgmine:

85	92	9D	57	D9	40	76	7A	97	89	E6	32	DC	07	BA	70

3DESKey1-le uue väärtuse seadmiseks toimime nii:

1) Valime juurkataloogi ja seejärel faili FID=0010:

CLA	INS	P1	P2
00	A4	00	0C

CLA	INS	P1	P2	Lc	FID	
00	A4	02	0C	02	00	10

2) Seame kaardisisese turvakeskkonna nr 2:

CLA	INS	P1	P2
00	22	F3	02

3) Saadame kaardile käsu GET CHALLENGE, et saada kutsung, mis koosneb kaheksast juhuslikult genereeritud baidist:

CLA	INS	P1	P2	Le
00	84	00	00	08

Märkus: Siit alates ei ole see näide enam täpselt korratav, kuna kaardi poolt väljastatav kutsung on iga kord erinev.

Näites kasutatud juhul vastas kaart järgmiselt:

Kutsung								OK trailer	
06	F3	22	BD	D4	84	88	A3	90	00

4) Järgmisena genereerime 2 juhuslikku väärtust, millest esimene – RND_IFD – on 8 baiti pikk ja teine – K_IFD – on 32 baiti pikk. Olgu meie näites need väärtused

RND_IFD = **01 02 03 04 05 06 07 08**

ja

K_IFD = **11 12 13 14 15 16 17 18**
21 22 23 24 25 26 27 28
31 32 33 34 35 36 37 38
41 42 43 44 45 46 47 48

Märkus: Praktikas töötavad rakendused peavad maksimaalse turvalisuse tagamiseks kasutama paremaid juhuslike väärtuste genereerimise meetodeid.

5) Moodustame bloki RND_IFD || Kaardilt saadud kutsung || K_IFD, meie näites:

RND_IFD, 8 baiti	Kaardi kutsung, 8 baiti	K_IFD, 32 baiti
01…08	06…A3	11..48

6) Krüptime selle bloki momendil kehtiva 3DESKey1-ga (see on tuletatud paroollausest “Kaks kurja kukke kaklevad kuudi katusel.”) 3DES CBC režiimis, kusjuures ICV=”00 00 00 00 00 00 00 00”. Tulemus on:

F2 89 C9 96 5D 10 DC DE
8E 88 58 10 FB D6 3D C5
9B E6 2E 20 D7 36 1E 8C
B5 C8 BB C7 1F E4 C9 D5
74 10 C1 7D 10 E9 F4 E8
F3 FF 7E D5 AE A8 90 17

7) Moodustame käsu MUTUAL AUTHENTICATE ja saadame kaardile. P2 = võtme number, mis 3DESKey1 puhul on 04:

CLA	INS	P1	P2	Lc	Moodustatud blokk	Le
00	82	00	04	30	F2…17	30

Kaart vastab järgmiselt:

Vastusblokk, 0x30 baiti	**OK trailer**	
….	**90**	**00**

Meie näites on vastusblokk järgmine:

2B 4A 0B E2 2B CF 2B FD
C1 ED 73 FA 5F D8 FE F2
74 D0 17 BA AB 48 DA 29
41 FF B8 33 47 2C 77 35
3B 56 C3 5A EA B6 31 70
52 D5 EA 6A 45 CA C4 5E

8) Vastusblokk on krüptitud 3DESKey1-ga 3DES CBC-režiimis, kus ICV=”00 00 00 00 00 00 00 00”. Dekrüptime selle bloki, tulemus on järgmine:

06 F3 22 BD D4 84 88 A3
01 02 03 04 05 06 07 08
69 DA 9F 6F F4 27 A7 8B
B6 8B DB B7 7A C7 89 43
6F 33 DB B5 9D 79 9F F2
C1 AB EA 1B B8 44 81 48

9) Sooritame järgmise operatsiooni:

(K_IFD) XOR (dekrüptitud vastusblokk[0x10..0x2F])

seega, XOR-me K_IFD dekrüptitud vastusbloki baitidega 16(dec)…47(dec). Tulemus on järgmine:

78 C8 8C 7B E1 31 B0 93 97 A9 F8 93 5F E1 AE 6B
5E 01 E8 81 A8 4F A8 CA 80 E9 A9 5F FD 02 C6 00

Siinkohal olemegi saanud esmase tulemuse – on tuletatud 2 EstEID turvalise kommunikatsiooni sessioonivõtit ja 8-baidine sõnumiloendur (ik '*send sequence counter*').

Ülaltoodud tabeli ülemine rida, "78…6B" on sessioonivõti1 – SK1 – ja alumine rida "5E…00" on sessioonivõti2 – SK2.

Sõnumiloenduri algväärtuse saame järgmiselt: sõnumiloenduri baidid 0..3 on kaardilt saadud dekrüptitud vastusbloki (vt punkt 8 eelpool) baidid 0xC kuni 0x10 ja sõnumiloenduri baidid 4..7 on sama bloki baidid 4..7. Seega on sõnumiloendur meie näites:

SSC = **05 06 07 08 D4 84 88 A3**

Järgnevalt võime asuda operatsiooni sooritamisele EstEID turvakommunikatsiooni all.

10) Sõnumiloendurit tuleb suurendada ühe võrra **enne iga** sessioonivõtmetega sooritatavat operatsiooni. **Sõnumiloenduri noorim bait on kõige parempoolsem**. Seega, suurendades sõnumiloendurit ühe võrra, saame

SSC = **05 06 07 08 D4 84 88 A4**

11) Moodustame faili FID=0010 kirje nr 1 ülekirjutamise käsu sarnaselt juhule, kui autoriseeritakse PIN2 abil:

CLA	INS	P1	P2	Lc	Võtme ID		Võtme väärtus uuest paroollauses "Kured läinud – kurjad ilmad."														
00	DC	01	04	12	04	00	85	92	9D	57	D9	40	76	7A	97	89	E6	32	DC	07	BA	70

Seda käsku ei saa aga saata otse kaardile. Andmevälja (so 'Võtme ID' + 'Võtme väärtus') tuleb töödelda sessioonivõtmete ja sõnumiloenduriga.

12) Selle käsu andmeväli tuleb krüptida 3DES algoritmiga. Selleks tuleb lisada blokile lõppu bait 0x80 ja seejärel nii mitu nullbaiti, et baitide arv blokis oleks 8 kordne.

Märkus: Kui bloki pikkus on kaheksa kordne juba ilma täiendavaid baite lisamata, siis lisame 8 baiti: "80 00 00 00 00 00 00 00".

Käesoleval juhul nii:

04	00	85	92	9D	57	D9	40	76	7A	97	89	E6	32	DC	07	BA	70	**80**	**00**	**00**	**00**	**00**	**00**

13) Järgnevalt krüptime selle bloki SK1-ga 3DES CBC režiimis, kusjuures ICV-na kasutame sõnumiloendurit. Tulemus on:

08	BB	57	9A	AB	1B	A2	B5	D5	BB	1E	83	16	F0	AC	F8	94	DD	24	7F	CF	16	F9	FB

14) Konstrueerime punktis 11 moodustatud käsu uuesti järgmiselt:

CLA	INS	P1	P2	Lc	Püsiväärtus	Järgneva bloki pikkus	Püsiväärtus	Eelmises punktis saadud krüptoblokk
0C	**DC**	**01**	**04**	**Lahtine**	**87**	**19**	**01**	**08…FB**

NB! CLA bait = 0x0C, mis tähendab, et käsus kasutatakse turvakommunikatsiooni.

15) Moodustame ajutiselt järgmise bloki:

Käsu päis, laiendatud pikkuseni 8 baiti || **Käsu andmeväli, laiendatud pikkuseni, mis on 8 kordne**

Antud juhul seega:

0C	DC	01	04	**80**	**00**	**00**	**00**
87	19	01	08	BB	57	9A	AB
1B	A2	B5	D5	BB	1E	83	16
F0	AC	F8	94	DD	24	7F	CF
16	F9	FB	**80**	**00**	**00**	**00**	**00**

16) Arvutame saadud bloki MAC-koodi 3DES CFB režiimis, kasutades võtmena SK1 ja ICV-na sõnumiloendurit. Tulemus on:

MAC = **87 94 E4 7E E2 CB 00 1F**

17) Moodustame lõpliku käsu, lisades punktis 14 koostatule arvutatud MAC-koodi ning seades paika Lc väärtuse. Vajadusel (kasutades T=1 protokolli) lisame ka Le, **mis on alati 0**:

CLA	INS	P1	P2	Lc	Püsi-väärtus	Järgneva bloki pikkus	Püsi-väärtus	Punktis 13 saadud krüptoblokk	Püsi-väärtus	Püsi-väärtus	Arvutatud MAC-kood	Le
0C	DC	01	04	**25**	87	19	01	08…FB	**8E**	**08**	**87..1F**	**0**

Selle käsu saadame kaardile.

Kaart vastab:

Püsiväärtused		OK Trailer'		Püsiväärtused		Vastuse MAC								OK Trailer	
99	**02**	**90**	**00**	**8E**	**08**	**51**	**CB**	**48**	**70**	**4D**	**6C**	**DA**	**4C**	**90**	**00**

OK Trailer "90 00" näitab, et turvakommunikatsioon töötas korrektselt, OK Trailer "90 00" näitab, et ka turvakommunikatsiooni all edastatud kaardi käsk töötas korrektselt.

Järgnevalt seisab ees kaardilt saadud vastuse autentsuse kontroll vastuse MAC-koodi abil. Selleks:

18) Suurendame ühe võrra sõnumiloendurit:

SSC = **05 06 07 08 D4 84 88 A5**

19) Laiendame vastuses sisaldunud andmed pikkuseni, mis on 8 kordne:

99 02 90 00 **80 00 00 00**

20) Arvutame selle bloki MAC-koodi 3DES CFB režiimis, kasutades võtmena SK1 ja ICV-na sõnumiloendurit (analoogselt punktis 16 tehtule). Tulemus on:

MAC = **51 CB 48 70 4D 6C DA 4C**

Seega võrdub arvutatud MAC-kood kaardilt saadud MAC-koodiga.

Sellega on paroollause1 asendamine, autoriseerides senise paroollausega, edukalt lõpule viidud. Uus paroollause on “Kured läinud - kurjad ilmad.”

Paroollause2 asendamine senise paroollausega autoriseerides toimub analoogselt järgmiste variatsioonidega:

1. Sessioonivõtmete ja sõnumiloenduri tuletamine toimub 3DESKey2 abil, mille järjekorranumber EstEID kaardil on 5 (P2 = 5 punktis 7)
2. Üle kirjutada tuleb kirje nr 2, st P1 = 2 punktis 11 moodustatud käsus.

Märkus: Viga sessioonivõtmete ja sõnumiloenduri tuletamisel (näiteks vale võtme kasutamine host-rakenduses) viib vastava 3DESKey valesisestuste loenduri vähenemisele ühe võrra. Loenduri algväärtus on 0xFF ning loendurit uuendada ei ole võimalik. Kui loenduri väärtus on jõudnud nulli, ei ole selle paroollausega autoriseerimist enam võimalik kasutada.

3DESKey valekasutuskordade loendurite väärtuste kaardilt lugemise kohta vaata juhendi esimesest osast.

14.4. Operatsioonide teostamine paroollausega autoriseerides

Nende operatsioonide teostamine paroollausega autoriseerides on analoogne paroollause seadmisele senise paroollausega autoriseerides (vt punkt 3.3.1), koosnedes järgmistest sammudest:

1. Tuletatakse sessioonivõtmed ja sõnumiloendur vastavast 3DESkey-st.
2. Konstrueeritakse käsk analoogselt PIN-koodiga autoriseerimise juhule.
3. Turvatakse see käsk sessioonivõtmete ja sõnumiloenduriga.
4. Saadetakse käsk kaardile ning loetakse vastus.
5. Kontrollitakse vastuse autentsust.

Allpool vaatleme iga operatsiooni näite varal eraldi.

Järgnev tabel näitab, missugust paroollauset tuleb erinevateks operatsioonideks kasutada:

	SSL-kutsungile vastuse arvutamine	Elektronallkirja arvutamine	Sessioonivõtme dekrüptimine autentimisvõtmega	Sessioonivõtme dekrüptimine allkirjavõtmega
Paroollause1	Jah		Jah	
Paroollause2		Jah		Jah

14.4.1. SSL-kutsungile vastuse arvutamine

Olgu meil paroollause1 “Kured läinud - kurjad ilmad” ning SSL-kutsung “30 31 32 33 34 35 36 37 38 39” (kasutame siin ülevaatlikkuse huvides lühendatud kutsungit).

Paroollausest tuletatud 3DESKey1 on, nagu eelmises peatükis arvutatud:

85	**92**	**9D**	**57**	**D9**	**40**	**76**	**7A**	**97**	**89**	**E6**	**32**	**DC**	**07**	**BA**	**70**

1) Seame turvakeskkonna 2 nii juurkataloogis kui EEEE kataloogis. Selleks:

Valime juurkataloogi:

CLA	INS	P1	P2
00	A4	00	0C

Seame kaardisisese turvakeskkonna nr 2:

CLA	INS	P1	P2
00	22	F3	02

Valime kataloogi EEEE:

CLA	INS	P1	P2	Lc	FID	
00	A4	01	0C	02	EE	EE

Seame **uuesti** kaardisisese turvakeskkonna nr 2:

CLA	INS	P1	P2
00	22	F3	02

2) Tuletame sessioonivõtmed SK1, SK2 ja sõnumiloenduri SSC sarnaselt peatükis 3.3.2 “Paroollause seadmine senise paroollausega autoriseerides” tehtuga, vt punktid 3..9.

Märkus: Siit alates ei ole see näide enam täpselt korratav, kuna tuletatud sessioonivõtmed SK1, SK2 ja sõnumiloendur SSC on iga kord erinevad..

Olgu selles näites

SK1 = **BA DA 02 DE 36 FB A7 BE 17 1D 8E A8 77 22 0D 78**

SK2 = **44 76 34 30 52 2B 5D A3 76 90 84 B2 DD F4 60 37**

ja SSC = **05 06 07 08 F9 2D E6 B3**

3) Suurendame sõnumiloendurit ühe võrra:

SSC = **05 06 07 08 F9 2D E6 B4**

4) Lisame kutsungile paremalt baidi 0x80 ja seejärel nii mitu nullbaiti, et saadud bloki pikkus oleks 8 kordne.

Märkus: Kui kutsungi bloki pikkus on kaheksa kordne juba ilma täiendavaid baite lisamata, siis lisame ikkagi 8 baiti: “80 00 00 00 00 00 00 00”.

Antud juhul saame:

30	31	32	33	34	35	36	37	38	39	80	00	00	00	00	00

5) Krüptime selle bloki 3DES CBC režiimis võtmega SK1, kusjuures ICV-na kasutame sõnumiloendurit (mida sai punktis 3 ühe võrra suurendatud). Tulemuseks saame:

29	5E	DE	E3	41	2A	82	30	0E	F8	74	C8	23	7E	6C	CD

6) Moodustame käsubloki järgnevalt:

Püsi-väärtus	Järgnevate andmete pikkus	Püsi-väärtus	Eelmisel sammul saadud blokk, pikkus 0x10 baiti	Püsi-väärtus	Püsi-väärtus	Püsi-väärtus
87	11	01	29…CD	97	01	80

Lõppu lisatud baidid “97 01 80” tähendavad, et oodatav vastuse pikkus on 0x80 baiti – 1024-bitine RSA krüptoblokk.

7) Moodustame SSL-kutsungile vastuse arvutamise käsu päise. See on analoogne PIN1-ga autoriseerimisel kasutatava käsu päisega, erinedes vaid CLA baidi osas, mille väärtus on 0x0C:

CLA	INS	P1	P2
0C	88	00	00

8) Moodustame ajutiselt järgmise bloki:

Käsu päis, laiendatud pikkuseni 8 baiti || **Sammul 6 moodustatud andmeväli, laiendatud pikkuseni, mis on 8 kordne**

Meie näites:

Päis	Päise laiendus pikkuseni 8	Sammul 6 saadud blokk	Sammul 6 saadud bloki laiendus pikkuseni, mis on 8 kordne
0C 88 00 00	80 00 00 00	87…80	80 00

9) Arvutame eelmisel sammul saadud bloki MAC-koodi 3DES CFB režiimis, kasutades võtmena SK2 ja ICV-na sõnumiloendurit. Tulemus on:

MAC = **20 10 A7 C3 10 84 A0 59**

10) Koostame käsu kaardile saatmiseks. Kui protokoll on T=1, tuleb lõppu lisada ka **Le=0**:

CLA	INS	P1	P2	Lc	Püsi-väärtus	Järgneva bloki pikkus	Püsi-väärtus	Punktis 5 saadud krüptoblokk	Püsi-väärtus	Püsi-väärtus	Arvutatud MAC-kood	Le
0C	88	00	00	20	87	11	01	29…CD	8E	08	20..59	00

Kaart vastab:

Püsiväärtused				Krüptitud kutsungivastus, 0x88 baiti	Püsiväärtused		MAC, 8 baiti	OK Trailer
87	81	89	01	….	8E	08	1E E7 D9 C2 42 41 D6 63	90 00

EstEID kaart lisab kaardilt väljasaadetavatele krüptitud andmeobjektidele samasuguse pikenduse (et pikkus oleks 8 kordne) kui tuleb lisada kaardile saadetavatele objektidele (vt punkt 4 ülalpool). Kuna kutsungivastuse pikkus on 0x80 baiti, mis on 8 kordne, siis lisab kaart sellele lõppu veel 8 baiti: “80 00 00 00 00 00 00 00”.

Järgnevalt tuleb kontrollida kaardilt saadud vastuse autentsust, arvutades MAC-koodi ning võrreldes seda kaardilt saabunud MAC-koodiga.

11) Suurendame sõnumiloendurit ühe võrra:

SSC = **05 06 07 08 F9 2D E6 B5**

12) Moodustame kaardilt saabunud vastusest ajutiselt järgmise bloki, kust jätame lõpust ära MAC-objekti (tagi 0x8E, pikkuse 0x08 ja MAC väärtuse) ning lisame selle asemele “80 00 00 00”, et saadud bloki pikkus oleks 8 kordne.

Püsiväärtused				Krüptitud kutsungivastus, pikkus 0x88 baiti	Püsiväärtused
87	81	89	01	….	80 00 00 00

13) Arvutame eelmisel sammul saadud bloki MAC-koodi 3DES CFB režiimis, kasutades võtmena SK2 ja ICV-na sõnumiloendurit. Meie näites on tulemus:

MAC = **1E E7 D9 C2 42 41 D6 63**

See on võrdne kaardilt saabunud MAC-koodiga.

14) Dekrüptime kutsungivastuse võtmega SK1 3DES CBC režiimis. Tulemus on järgmine:

Kutsungivastus, pikkus 0x80 baiti	Laiendus pikkusega 8 baiti
….	80 00 00 00 00 00 00 00

Jätame lõpust laienduse ära ning arvutatud kutsungivastus ongi käes.

14.4.2. Elektroonse allkirja arvutamine

Elektroonse allkirja arvutamine paroollausega autoriseerides on sarnane SSL-kutsungile vastuse arvutamisega. Erinevused on järgmised:

1) Kasutada tuleb paroollauset2 (3DESKey2); katse autoriseerida paroollause1-ga viib veasituatsiooni.

2) Käsu päis on järgmine (vt punkt 7 peatükis 3.4.1):

CLA	INS	P1	P2
0C	2A	9E	9A

ning (turvamata) andmeväljale tuleb kutsungi asemele paigutada räsiobjekt (vt punkt 4 peatükis 3.4.1).

Loe elektroonse allkirja arvutamise kohta ka juhendi esimese osa peatükist 11.1 “Elektronallkirja arvutamine, kui räsi on valmis”[7].

14.4.3. Sessioonivõtmete dekrüptimine

Ka sessioonivõtme dekrüptimise käskude turvamine paroollausega autoriseerimise korral on analoogne SSL kutsungile vastuse ja elektronallkirja arvutamise käskude turvamisega, kuid siiski mitmete määravate nüanssidega. Seetõttu vaatleme seda operatsiooni lähemalt.

Sessioonivõtme dekrüptimiseks autentimisvõtmega tuleb autoriseerimiseks kasutada paroollauset1 ja dekrüptimisel signeerimisvõtmega tuleb autoriseerimiseks kasutada paroollauset2. Vastupidine viib veasituatsiooni.

Olgu meie paroollause2 “See on minu paroollause2.” Ja sessioonivõtit sisaldav krüptoblokk pikkusega 0x80 baiti järgmine:

21 A6 … B9 E1

Paroollausest tuletatud 3DESKey2 on, nagu peatükis 3.2 arvutatud:

[7] Elektronallkirja arvutamise võimaluse kohta paroollausega autoriseerides ja kasutades räsimist kaardil, info puudub. Samas puudub ka nähtav vajadus selle operatsiooni järele, sest paroollauset kasutatakse suuremates, täisklaviatuuriga seadmetes, kus räsifunktsioon on olemas süsteemses tarkvaras ning kaardil räsimiseks puudub vajadus.

30	A1	DB	94	DF	29	BC	65	A8	17	25	2B	A6	73	88	FE	9B	7B	D6	43

1) Seame **turvakeskkonna 2 juurkataloogis ja turvakeskkonna 7 EEEE kataloogis**. Selleks:

Valime juurkataloogi:

CLA	INS	P1	P2
00	A4	00	0C

Seame kaardisisese turvakeskkonna **nr 2**:

CLA	INS	P1	P2
00	22	F3	02

Valime kataloogi EEEE:

CLA	INS	P1	P2	Lc	FID	
00	A4	01	0C	02	EE	EE

Seame kaardisisese turvakeskkonna **nr 7**:

CLA	INS	P1	P2
00	22	F3	07

2) Järgnevalt tuleb modifitseerida kaardisisest turvakeskkonda. Need operatsioonid on analoogsed sessioonivõtme dekrüptimisega PIN-koodiga autoriseerides (vt juhendi esimese osa peatüki 12 punktid 4..6).

Modifitseerime kaardisisest turvakeskkonda, kustutades viida autentimisvõtmele, st ütleme kaardile, et autentimise operatsioone ei ole järgnevalt vaja teha:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	A4	02	83 00

Modifitseerime kaardisisest turvakeskkonda, kustutades viida signeerimisvõtmele, st ütleme kaardile, et signeerimise operatsioone ei ole järgnevalt vaja teha:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	B6	02	83 00

Modifitseerime kaardisisest turvakeskkonda, seades viida võtmele, millega soovime dekrüptimise operatsiooni sooritada. Kui soovime dekrüptida signeerimisvõtmega, saadame järgneva käsu[8]:

CLA	INS	P1	P2	Lc	Võtmeviit
00	22	41	**B8**	05	83 03 80 **01 00**

Märkus: Autentimisvõtmega dekrüptimiseks oleks võtmeviit "83 03 80 ***11 00".***

3) Tuletame sessioonivõtmed SK1, SK2 ja sõnumiloenduri SSC sarnaselt peatükis 3.3.2 "Paroollause seadmine senise paroollausega autoriseerides" tehtuga, vt punktid 3..9. Kasutada tuleb 3DESKey2, st võtme järjekorranumber EstEID kaardis on **5** (3DESKey1 korral 4).

[8] Sellisel kujul on see käsk siis, kui kaardil ei ole pärast personaliseerimist genereeritud uut võtmepaari. Kuidas toimida siis, kui sellist eeldust ei ole võimalik kasutada, vaata järgmisest peatükist.

Olgu selles näites

SK1 = **EB 08 02 E5 4A 25 07 2B B6 98 33 6F 6C B3 E9 E5**

SK2 = **D9 B1 E7 B0 04 21 4F 42 E8 8D 9D CD 50 1D FD 82**

ja SSC = **05 06 07 08 B6 E4 C8 2C**

4) Suurendame sõnumiloendurit ühe võrra:

SSC = **05 06 07 08 B6 E4 C8 2D**

5) Lisame krüptoblokile ette (vasakule) ühe nullbaidi, nii et bloki pikkus on nüüd 0x81 baiti:

00 21 A6 … B9 E1

6) Lisame kutsungile paremalt baidi 0x80 ja seejärel nii mitu nullbaiti, et saadud bloki pikkus oleks 8 kordne. Kuna eelmine operatsioon andis bloki pikkuseks 0x81 baiti, siis selle operatsiooni tulemusena on blokk selline

1 nullbait	Krüptoblokk, pikkus 0x80 baiti	Laiendus
00	21 A6 …B9 E1	80 00 00 00 00 00 00

7) Krüptime selle bloki 3DES CBC režiimis võtmega SK1, kusjuures ICV-na kasutame sõnumiloendurit (mida sai punktis 4 ühe võrra suurendatud). Tulemusena saame:

Krüptitud blokk, pikkus 0x88 baiti
36 0D … E2 53

8) Moodustame käsubloki järgnevalt:

Püsiväärtused	Eelmisel sammul saadud blokk, pikkus 0x88 baiti	Püsi-väärtus	Püsi-väärtus	Püsi-väärtus (Le')
87 81 89 01	36 0D…E2 53	97	01	00

Lõppu lisatud baidid "97 01 00" tähendavad, et oodatav vastuse pikkus ei ole teada ja seega antakse pikkuse väärtuseks 0. Krüptoblokis sisaldub tavaliselt SSL sessiooni andmete krüptimise salajase võtme ASN.1 järgi kodeeritud objekt, kusjuures kasutada võidakse väga mitmesuguseid ja erineva võtmepikkusega krüptoalgoritme. Seetõttu ei ole võimalik ette teada krüptoblokis sisalduva võtmeobjekti pikkust ning kaardilt oodatavate andmete pikkuseks seatakse Le'=0.

9) Moodustame SSL-kutsungile vastuse arvutamise käsu päise. See on analoogne PIN1-ga autoriseerimisel kasutatava käsu päisega, erinedes vaid CLA baidi osas, mille väärtus on 0x0C:

CLA	INS	P1	P2
0C	2A	80	86

10) Moodustame ajutiselt järgmise bloki:

Käsu päis, laiendatud pikkuseni 8 baiti || **Sammul 8 moodustatud andmeväli, laiendatud pikkuseni, mis on 8 kordne**

Meie juhul:

Päis	Päise laiendus pikkuseni 8	Sammul 8 saadud blokk	Sammul 8 saadud bloki laiendus pikkuseni, mis on 8 kordne
0C 2A 80 86	**80 00 00 00**	**87 81 89 01 36 … 53 97 01 00**	**80**

11) Arvutame eelmisel sammul saadud bloki MAC-koodi 3DES CFB režiimis kasutades võtmena SK2 ja ICV-na sõnumiloendurit. Antud juhul on tulemus:

MAC = **53 2B 42 7E 06 87 29 7A**

12) Koostame käsu kaardile saatmiseks. Kui protokoll on T=1, siis tuleb lõppu lisada ka **Le=0**:

CLA	INS	P1	P2	Lc	Püsiväärtused	Punktis 7 saadud krüptoblokk, pikkus 0x88	Püsi-väärtused	Arvutatud MAC-kood	Le
0C	**2A**	**80**	**86**	**99**	**87 81 89 01**	**36 0D … E2 53**	**8E 08**	**53..7A**	**0**

Kaart vastab:

Püsi-väärtus	Järgneva andmebloki pikkus	Püsi-väärtus	Krüptitud sessioonivõti	Püsi-väärtused		MAC, 8 baiti	OK Trailer
87	**11**	**01**	**F7 32 40 48 18 D5 67 96 26 1E 5B B8 6C BB 4D 14**	**8E**	**08**	**60 19 E8 61 7C 6D 88 25**	**90 00**

Järgnevalt tuleb kontrollida kaardilt saadud vastuse autentsust, arvutades MAC-koodi ning võrreldes seda kaardilt saabunud MAC-koodiga.

13) Suurendame sõnumiloendurit ühe võrra:

SSC = **05 06 07 08 B6 E4 C8 2E**

14) Moodustame kaardilt saabunud vastusest ajutiselt järgmise bloki: jätame lõpust ära MAC-objekti (tagi 0x8E, pikkuse 0x08 ja MAC väärtuse) ning lisame selle asemele “80 00 00 00 00”, et saadud bloki pikkus oleks 8 kordne.

Püsiväärtused			Krüptitud sessioonivõti	Püsiväärtused
87	**11**	**01**	**F7 32 40 48 18 D5 67 96 26 1E 5B B8 6C BB 4D 14**	**80 00 00 00 00**

15) Arvutame eelmisel sammul saadud bloki MAC-koodi 3DES CFB režiimis, kasutades võtmena SK2 ja ICV-na sõnumiloendurit. Meie juhul on tulemus:

MAC = **60 19 E8 61 7C 6D 88 25**

16) Dekrüptime kaardilt saadud andmebloki, kasutades 3DES-võtmena SK1 ja ICV-na sõnumiloendurit. Tulemuseks saame:

30 31 32 33 34 35 36 37 38 39 80 00 00 00 00 00

17) Jätame lõpust ära laienduse, saame sessioonivõtme objekti väärtuseks ASCII kujul “0123456789”.

15. Sessioonivõtme dekrüptimine juhul, kui kaardil on pärast personaliseerimist genereeritud uus võtmepaar

EstEID kaardil on võimalik genereerida uus RSA võtmepaar nii autentimisvõtmele kui ka signeerimisvõtmele. Käesoleva juhendi koostamise hetkel ei olnud teada, kas üldse ja kui, siis mis asjaoludel hakatakse kaartidel uusi võtmepaare genereerima, kuid selline tehniline võimalus on olemas (võtmepaaride genereerimise protseduuri enese kohta vt peatükki 6.3 selles juhendis).

SSL-kutsungile vastuse arvutamise protseduur ja elektronallkirja arvutamise protseduur ei muutu sellest, kui kaardil genereeritakse uus võtmepaar, sest võtmete genereerimisel või uute sertifikaatide laadimisel muudetakse kaardil ka võtmeviitasid. Sessioonivõtme dekrüptimise operatsioonidel see aga nii ei ole. Kui ei ole võimalik eeldada, et kaardil pärast personaliseerimist uusi võtmeid genereeritud ei ole, siis tuleb enne dekrüptimisoperatsiooni teostamist sooritada mõned lisaoperatsioonid.

EstEID kaardil on järgmised võtmepaarid:

Võtme ID (HEX BCD)	Kirjeldus
0100	Signeerimisvõti1
1100	Autentimisvõti1
0200	Signeerimisvõti2
1200	Autentimisvõti2

Kaardi personaliseerimisel genereeritakse Autentimisvõti1 ja Signeerimisvõti1 ning Signeerimisvõti2 ja Autentimisvõti2 jäävad tühjaks (nende poole pöördumine viib veasituatsiooni).

Kui nüüd genereeritakse uued võtmepaarid, siis paigutatakse uued salajased võtmed vastavalt Autentimisvõti2 ja Signeerimisvõti2 kohtadele ning senised võtmed säilivad. Järgmisel genereerimisel paigutatakse uued salajased võtmed Signeerimisvõti1 ja Autentimisvõti1 kohtadele ning senised võtmed säilivad kohtadel Signeerimisvõti1 ja Autentimisvõti1. Personaliseerimisel moodustatud võtmed viimasel operatsioonil hävivad. Uute võtmepaaride genereerimise kordade arv piiratud ei ole.

Kataloogi EEEE failis FID=0033 on kirjas, missugused võtmed momendil kehtivad. See on struktureeritud fail ning sisaldab ühe kirje, mis pärast personaliseerimist on järgmine:

Bait nr	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**	**10**	**11**	**12**	**13**	**14**
Väärtus	**00**	**A4**	**08**	**95**	**01**	**40**	**83**	**03**	**80**	**11**	**00**	**B6**	**08**	**95**	**01**	**40**	**83**	**03**	**80**	**01**	**00**

Jooksva autentimisvõtme viit on baitides nr 9..A ja signeerimisvõtme viit baitides nr 0x13..0x14.

Selleks, et sooritada dekrüptimise operatsioon võtme jooksva versiooniga, tuleb esmalt teha kindlaks, missugune võtmetest on jooksev, lugedes kirje nr 1 failist EEEE/0033. Seejärel tuleb modifitseerida kaardisisest turvakeskkonda, öeldes kaardile, et operatsioon tuleb teostada just selle võtmega.

Seega tuleb juhendi esimeses osas peatükis 12 “Sessioonivõtme dekrüptimine” toodud protseduuri punkti 6 täiendada ning sõnastada see nii:

6) Modifitseerime kaardisisest turvakeskkonda, seades viida võtmele, millega soovime dekrüptimise operatsiooni sooritada.

   Loeme kirje nr 1 failist FID=0033.

   Kui soovime dekrüptida autentimisvõtmega, saadame järgneva käsu:

CLA	INS	P1	P2	Lc	Võtmeviit		
00	22	41	**B8**	05	83 03 80	Bait nr 9 kirjest nr 1 failis EEEE/0033	Bait nr A kirjest nr 1 failis EEEE/0033

Kui soovime dekrüptida signeerimisvõtmega, saadame järgneva käsu:

CLA	INS	P1	P2	Lc	Võtmeviit		
00	22	41	**B8**	05	83 03 80	Bait nr 0x13 kirjest nr 1 failis EEEE/0033	Bait nr 0x14 kirjest nr 1 failis EEEE/0033

Sama kehtib ka siis, kui kasutaja autoriseeritakse paroollausega.

16. Operatsioonid võtmete eelmiste versioonidega

EstEID kaardil on võimalik sooritada operatsioone võtmete eelmiste versioonidega. Need protseduurid on sarnased jooksvate võtmetega sooritatavate vastavate operatsioonidega, kuid lisaks tuleb failist EEEE/0033 lugeda välja, missugune on võtme jooksev versioon ning modifitseerida kaardisisest turvakeskkonda, seades viidad võtme eelmisele versioonile.

16.1. SSL-kutsungile vastuse arvutamine võtme eelmise versiooniga

SSL-kutsungile vastuse arvutamisel autentimisvõtme eelmist versiooni kasutades tuleb toimida nii (vt ka peatükki 10 “SSL kutsungile vastuse arvutamine” juhendi I osas):

1) Valime juurkataloogi.
2) Valime kataloogi EEEE.
3) Seame kaardisisese turvakeskkonna nr 1.
4) **Loeme kirje nr 1 failist FID=0033.**
5) **Seame võtmeviida käsuga**

CLA	**INS**	**P1**	**P2**	**Lc**	**Võtmeviit**	
00	**22**	**41**	**A4**	**05**	**83 03 80**	**Võtmeviida väärtus**

Kui baidid nr 9 ja A failist FID=0033 on ”1100”, siis on seatava võtmeviida väärtuseks “1200” ja vastupidi, et saavutada võtme mittejooksva versiooni kasutamine operatsiooni sooritamiseks.

6) Verifitseerime PIN1.
7) Saadame kaardile käsu kutsungi vastuse arvutamiseks:

CLA	INS	P1	P2	Lc (kutsungi pikkus)	Kutsung	Le
00	88	00	00	24	….	80

8) Kaardi vastuse vorming ei erine jooksva võtmega sooritatud operatsioonil saadava vastuse omast.

Kui autoriseerimiseks kasutatakse paroollauseid, siis tuleb faili FID=EEEE/0033 lugemine ja võtmeviitade seadmine sooritada protseduuri punktide 1 ja 2 vahel (vt peatükki 3.4.1), st pärast turvakeskkondade seadmist ja enne sessioonivõtmete tuletamist.

16.2. Elektronallkirja arvutamine võtme eelmise versiooniga

Elektronallkirja arvutamiseks võtme eelmise versiooniga tuleb toimida järgmisel viisil (vt ka peatükki 11 “Elektronallkirja arvutamine” juhendi I osas):

1) Valime juurkataloogi.
2) Valime kataloogi EEEE.
3) Seame kaardisisese turvakeskkonna nr 1.
4) **Loeme kirje nr 1 failist FID=0033.**
5) **Seame võtmeviida käsuga**

CLA	INS	P1	P2	Lc	Võtmeviit	
00	**22**	**41**	**B6**	**05**	**83 03 80**	**Võtmeviida väärtus**

Kui baidid nr 0x13 ja 0x14 failist FID=0033 on ”0100”, siis on seatava võtmeviida väärtuseks “0200” ja vastupidi, et saavutada võtme mittejooksva versiooni kasutamine operatsiooni sooritamiseks.

6) Verifitseerime PIN2.
7) Saadame kaardile käsu elektronallkirja arvutamiseks:

CLA	INS	P1	P2	Lc (räsiobjekti pikkus)	Räsiobjekt	Le
00	2A	9E	9A	23	….	80

8) Kaardi vastuse vorming ei erine jooksva võtmega sooritatud operatsioonil saadava vastuse omast.

Kui autoriseerimiseks kasutatakse paroollauseid, tuleb faili FID=EEEE/0033 lugemine ja võtmeviitade seadmine sooritada (analoogselt SSL-kutsungile vastuse arvutamise protseduuriga) pärast turvakeskkondade seadmist ja enne sessioonivõtmete tuletamist.

16.4. Sessioonivõtme dekrüptimine võtme eelmise versiooniga

Kui soovitakse sooritada dekrüptimisoperatsioon võtme eelmise versiooniga, tuleb operatsioon sooritada samuti kui võtme jooksva versiooniga dekrüptimisel, kuid võtmeviit tuleb seada vastupidine sellele, mis on kirjas failis EEEE/FID=0033. Kui autentimisvõtme väärtus failis on “1100”, siis seame kaardis “1200” ja vastupidi. Kui signeerimisvõtme väärtus failis on “0100”, siis seame kaardis “0200” ja vastupidi.

17. Kaardihalduse operatsioonid

17.1. Operatsioonidest üldiselt

Kaardihaldusoperatsioonide all mõistetakse EstEID kiibiga sooritatavaid operatsioone, mis ei toimu kaardi kasutaja äranägemisel, vaid mille sooritamiseks annab loa Kaardihalduskeskus. Loa andmine realiseeritakse krüptograafiliste meetoditega.
Kaardihalduse süsteem võimaldab sooritada nelja tüüpi EstEID kaardiga seotud operatsioone:

1. **Sertifikaatide laadimiskoodide genereerimine** – selleks, et asendada EstEID kaardil sertifikaat, näiteks senise sertifikaadi kehtetuksmuutumise ja uue väljastamise tõttu, tuleb sertifikaat konverteerida erilisse nn laadimiskoodi. Laadimiskoode suudab genereerida vaid vastavat salajast võtit omav kaardihalduskeskus.

2. **Autoriseeringute andmine kaardile uute PIN-koodide seadmiseks juhul, kui kaardi PUK-kood on hävinud** – selle operatsiooni käigus seatakse kaardile uued PIN- ja PUK-koodid, kusjuures seniseid koode teada ei ole vaja. Kaardi valdaja isikusamasus tuvastatakse mitteelektrooniliste vahenditega ning operatsiooni

väärkasutuse vältimiseks on vajalik luua vastav organisatsiooniliste meetmete süsteem.

3. **Lisarakenduste kaardile laadimise moodulite genereerimine** – EstEID kaardile on võimalik laadida ka muid rakendusi, kuid see saab toimuda ainult vastavat pädevust omava institutsiooni loal. Tehniliselt kontrollib lisarakenduste laadimist Kaardihalduskeskus. EstEID kaart võtab lisarakendusi vastu ainult teatud protseduuri abil laadimiskoodi konverteeritult. Konverteerimise operatsiooni teostab Kaardihalduskeskus, kes omab vastavat salajast võtit.

4. **EstEID kaardil uute võtmepaaride genereerimiseks autoriseeringute andmine** – EstEID kaart võimaldab genereerida uusi salajaste võtmete paare. Uue võtmepaari genereerimine saab toimuda Kaardihalduskeskuse poolt autoriseerituna.

EstEID kaardihalduse süsteemi turvalisuse aluseks on neli salajast 3DES võtit:

CMK1 – kasutatakse PIN-koodide asendamiseks
CMK2a – kasutatakse uute võtmepaaride genereerimisel
CMK2b – kasutatakse sertifikaatide laadimismoodulite moodustamiseks ja võtmeviitade seadmiseks pärast võtmete genereerimist
CMK3 – kasutatakse lisarakenduste laadimismoodulite moodustamiseks.

Selles juhendis kasutatavad näidisvõtmed on järgmised:

CMK1 = A1A1A1A1A1A1A1A1A2A2A2A2A2A2A2A2
CMK2a = B0B0B0B0B0B0B0B0B3B3B3B3B3B3B3B3
CMK2b = C1C1C1C1C1C1C1C1C2C2C2C2C2C2C2C2
CMK3 = D0D0D0D0D0D0D0D0D3D3D3D3D3D3D3D3

17.2. Kaardikohaste võtmete tuletamine

Kuna 3DES on sümmeetriline krüptoalgoritm, siis peavad salajased võtmed olema kirjutatud ka igale EstEID kaardile. Turvakaalutlustel ei kirjutata kaartidele Kaardihalduskeskuses hoitavaid peavõtmeid, vaid peavõtmest ja kaardivaldaja isikukoodist tuletatud kaardikohased võtmed. Tuletamise protseduur on järgmine:

1. Arvutatakse kaardi kasutaja isikukoodi SHA-1 räsi.
2. Võetakse saadud räsist 16 vasakpoolset baiti.
3. Krüptitakse need baidid vastava peavõtmega 3DES CBC režiimis, kus ICV=”00 00 00 00 00 00 00 00”.
4. Seatakse iga baidi noorim bitt nii, et bait oleks paaritu.

Näide: Olgu kaardi kasutaja isikukood (ASCII) “01234567890”. Arvutame kaardikohased võtmed peatükis 6.1 toodud näidispeavõtmetega.

1. Selle isikukoodi SHA-1 räsi on:

   7E D1 0E 4A 58 9C 87 F9 E6 A8 5C 22 E4 B0 C3 8E CF 5F 50 59

2. Krüptime 16 vasakpoolset baiti võtmega CMK1 3DES CBC režiimis, ICV=0:

   41 F9 AE 35 48 53 6F 19 B9 3F ED 4E F8 90 C9 3B

3. Seame noorimad bitid nii, et baidid oleksid paaritud:

   Kaardi CMK1 = **40 F8** AE **34 49 52 6E** 19 B9 **3E EC 4F** F8 **91 C8** 3B

Samuti arvutame:

Kaardi CMK2a = 89 FB 5D 9B B0 83 D0 97 AB 13 5E BF 70 DF FD 86
Kaardi CMK2b = 3B 8A BC 9B 98 1F 29 AB B3 0D 97 15 64 29 43 62
Kaardi CMK3 = 6E DC 2A 25 D6 64 7C D0 C1 BF 01 16 08 51 F7 04

17.3. Uute võtmepaaride genereerimine

Uue võtmepaari genereerimine EstEID kaardil toimub nii:

1) Loeme kaardi kasutaja isikukoodi, mis on kirjas isikuandmete failis FID=EEEE/5044 kirjes nr 7. Olgu isikukoodiks (ASCII) 01234567890.

2) Loeme kirje 1 failist FID=EEEE/0033, et teada saada, missuguste viitadega võtmed on kaardis momendil jooksvad. Jooksva autentimisvõtme viit on loetud kirje baitides 0x9..0xA ja signeerimisvõtme viit baitides 0x13..0x14 (baitide loendus algab nullist). Uus võti tuleb genereerida sellesse võtmesse, mis pole momendil jooksev. Seega säilib jooksev võti juhuks, kui seda peaks hiljem vaja minema. Kui autentimisvõtme viit on failis FID=EEEE/0033 “1100”, siis genereeritava võtme viit on “1200” ja vastupidi. Kui signeerimisvõtme viit on failis FID=EEEE/0033 “0100”, siis genereeritava võtme viit on “0200” ja vastupidi. Tehniliselt pole ka takistust võtme jooksva versiooni ülegenereerimiseks.

3) Seame turvakeskkonna nr 3 nii juurkataloogis kui EEEE kataloogis:

Valime juurkataloogi:

CLA	INS	P1	P2
00	A4	00	0C

Seame kaardisisese turvakeskkonna nr 3:

CLA	INS	P1	P2
00	22	F3	03

Valime kataloogi EEEE:

CLA	INS	P1	P2	Lc	FID	
00	A4	01	0C	02	EE	EE

Seame **uuesti** kaardisisese turvakeskkonna nr 3:

CLA	INS	P1	P2
00	22	F3	03

4) Verifitseerime PIN1-koodi. PIN1-koodi verifitseerimine on mõeldud selleks, et tagada operatsiooni toimumine kaardi kasutaja teadmisel.

5) EstEID kaardi kataloogis EEEE on fail FID=EEEE/0013, milles hoitakse salajasi võtmeid puudutavat teeninduslikku infot[9]. See on fikseeritud kirjepikkusega struktureeritud fail (kirje pikkus 0x4F), milles sisaldub neli kirjet – iga kirje kuulub ühe salajase võtme juurde:

Võti	Võtme ID	Kirje nr failis FID=EEEE/0013
Signeerimisvõti1	0100	1

[9] Selles failis sisalduva info sisu kohta loe MICARDO 2.1 kasutusjuhendist.

Signeerimisvõti2	0200	2
Autentimisvõti1	1100	3
Autentimisvõti2	1200	4

Uue võtme genereerimist juhib kirje bait nr 0x32 (loendus algab nullist). Selle väärtused on autentimis- ja signeerimisvõtmetel erinevad:

Võti	**Baidi nr 0x32 väärtus faili FID=EEEE/0013 vastavas kirjes**	**Võtme olek**
Signeerimisvõti1 ja Signeerimisvõti2	**F6**	Võti puudub - tuleb genereerida.
	B6	Võti on genereeritud – tööks valmis.
Autentimisvõti1 ja Autentimisvõti2	**E4**	Võti puudub - tuleb genereerida.
	A4	Võti on genereeritud – tööks valmis.

Uue võtmepaari genereerimiseks tuleb selle baidi väärtus seada nii, et võtme genereerimine oleks lubatud. Seda on võimalik teha näiteks, lugedes selle kirje välja käsuga READ BINARY (kirjed on vabalt loetavad), muuta väljaloetud kirjes baidi nr 0x32 väärtus selliseks, et võtme genereerimine oleks lubatud ning kirjutada kirje siis tagasi faili.

Selleks aga, et kirje failis FID=EEEE\0013 üle kirjutada, on vaja Kaardihalduskeskuse autoriseeringut. Edasi toimime nii:

6) Moodustame käsu faili FID=EEEE\0013 kirje ülekirjutamiseks. Alljärgnev on käsk faili kirje nr 4 (puudutab Autentimisvõti2) ülekirjutamiseks:

Päis	Lc	Andmed
00 DC 04 04	4F	830412001012C00281809103FFFFFF7B 18800100A10A8B080030010302040305 **E4**07950140890221137B11800106A103 8B010BB807950140890211307B118001 07A1038B010CB80795014089021130

7) Muudame käsu päist järgnevalt:

Päis
0C DC 04 04

CLA = 0C tähendab, et käsk edastatakse EstEID kaardile turvalise kommunikatsiooni all. Sellel operatsioonil ei kasutata aga sessioonivõtmete tuletamist ega krüptimist. Arvutatakse vaid MAC-kood.

8) Moodustame järgmise bloki:

Püsiväärtus	Andmebloki pikkus = Lc	Andmeblokk
81	**4F**	83 04…11 30

9) Moodustame ajutiselt järgmise bloki:

Käsu päis	Käsu päise laiendus pikkuseni 8	Eelmisel sammul moodustatud blokk	Eelmisel sammul moodustatud bloki laiendus pikkuseni, mis 8 kordne
0C DC 04 04	80 00 00 00	81 4F 83 04…11 30	80 00 00 00 00 00 00

10) Arvutame selle bloki MAC-koodi 3DES CBC režiimis **kaardikohase võtmega CMK2b**, kus ICV=”00 00 00 00 00 00 00 00”. Meie juhul on tulemus:

9F 7F CD 8B 02 F8 56 C4

11) Moodustame järgmise käsu:

Päis	Lc	Sammul 8 moodustatud blokk	Püsiväärtused	Sammul 10 arvutatud MAC	Le
0C DC 04 04	5B	81 4F 83 04…11 30	8E 08	9F 7F CD 8B 02 F8 56 C4	00

12) Saadame selle käsu kaardile. Kui kasutatakse protokolli T=1, siis peab lõpus olema Le=0. Kaart vastab:

Püsiväärtused	OK Trailer’	Püsiväärtused	MAC	OK Trailer
99 02	**90 00**	8E 08	F9 5D 3F 23 71 D5 B7 11	**90 00**

Kui OK Trailer ja OK Trailer’ on mõlemad “90 00”, võime jätkata.

Märkus: Pärast seda operatsiooni ei ole käsitletav salajane võti enam kasutatav. Kui operatsioon edaspidi mingil põhjusel katkeb, tuleb seda uuesti otsast alustada.

Märkus: Sammul 11 moodustatud käsk on kasutatav korduvalt, kuna ei sisalda sessiooni-spetsiifilist elementi.

13) Järgnevalt tuletame sessioonivõtme analoogselt peatükis 3.3.2 punktides 3..9 tehtuga. 3DES võtmena kasutame kaardi **CMK2a**, mille kaardisisene järjekorranumber on **2**.

Olgu meie juhul:

SK1 = 95 CC 39 2F 24 38 AA 24 1F B9 DC F4 77 77 30 FD
SK2 = 30 FD B4 B6 7B A8 74 6E 0E 67 43 A3 72 90 E9 5D
SSC = 05 06 07 08 4E 56 55 CB

14) Võtme genereerimiseks on vajalikud spetsiifilised muudatused kaardisiseses turvakeskkonnas. Need muudatused on erinevad autentimisvõtme ja signeerimisvõtme genereerimiseks.

Autentimisvõtme genereerimisel seame turvakeskkonna nii:

a) Kustutame viida signeerimisvõtmele:

CLA	INS	P1	P2	Lc	Data
00	**22**	**41**	**B6**	**02**	**83 00**

b) Seame viida genereeritavale autentimisvõtmele:

CLA	INS	P1	P2	Lc	Data	
					Püsiväärtused	Võtmeviit
00	**22**	**41**	**A4**	**05**	**83 00 80**	**12 00**

Signeerimisvõtme genereerimisel seame turvakeskkonna nii:

a) Seame viida genereeritavale signeerimisvõtmele

CLA	INS	P1	P2	Lc	Data	
					Püsiväärtused	Võtmeviit
00	**22**	**41**	**B6**	**05**	**83 00 80**	**02 00**

b) Seame viida autentimisvõtmele:

CLA	INS	P1	P2	Lc	Data	
					Püsiväärtused	Võtmeviit
00	**22**	**41**	**A4**	**05**	**83 00 80**	**12 00**

Autentimisvõtme viida seadmine signeerimisvõtme genereerimisel on vajalik selleks, et EstEID kaart arvutab genereeritud avalikule võtmele allkirja, kasutades selleks nii autentimisvõtme kui signeerimisvõtme korral autentimisvõtit (autentimisvõtme korral seega iseennast). Seetõttu genereeritakse siis, kui uuendatakse mõlemaid võtmeid, esmalt autentimisvõti ja seejärel signeerimisvõti.

Märkus: Signeerimisvõtme genereerimisel tuleb seada viit varem genereeritud autentimisvõtmele. Viida seadmine autentimisvõtmele, mida pole kunagi genereeritud, viib veasituatsiooni.

15) Moodustame käsu võtme genereerimiseks:

CLA	INS	P1	P2	Lc	Püsiväärtused	Avaliku võtme faili FID (püsiväärtus)
00	**46**	**00**	**00**	**04**	**8302**	**1000**

Võtmepaari genereerimisel moodustatud avalik võti paigutub faili FID=1000.

Järgnevalt tuleb see käsk edastada kaardile EstEID turvakommunikatsiooni all, kasutades sammul 13 moodustatud sessioonivõtmeid ja sõnumiloendurit. Turvakommunikatsioonis kasutatakse ainult kaitset MAC-koodidega, krüptimist ei kasutata.

16) Suurendame sõnumiloendurit 1 võrra:

SSC = 05 06 07 08 4E 56 55 C**C**

17) Muudame käsu päist järgmiselt:

CLA	INS	P1	P2
0C	46	00	00

18) Moodustame ajutiselt järgmise bloki:

Päis	Päise laiendus pikkuseni 8	Andmed	Andmebloki laiendus pikkuseni 8
0C 46 00 00	**80 00 00 00**	81 04 83 02 10 00	**80 00**

19) Arvutame moodustatud bloki MAC-koodi kaardi võtmega CMK2b 3DES CFB režiimis, kus ICV="00 00 00 00 00 00 00 00". Tulemus on:

MAC = **2B 08 D5 EF B2 53 FC C6**

20) Moodustame käsu, mille saadame kaardile:

Päis	Lc	Püsiväärtused	Püsiväärtused	Püsiväärtused	Eelmisel sammul arvutatud MAC	Le
0C 46 00 00	10	81 04	83 02 10 00	8E 08	2B 08 D5 EF B2 53 FC C6	00

Kaart vastab:

Püsiväärtused	OK Trailer'	Püsiväärtused	MAC	OK Trailer
99 02	90 00	8E 08	69 CA B6 19 A6 EC 60 C9	90 00

Järgnvalt kontrollime saadud vastuse autentsust.

21) Suurendame sõnumiloendurit ühe võrra:

SSC = 05 06 07 08 4E 56 55 C**D**

22) Moodustame ajutiselt bloki:

Kaardi vastus	Kaardi vastuse laiendus pikkuseni 8
99 02 90 00	**80 00 00 00**

23) Arvutame moodustatud bloki MAC-koodi kaardi võtmega CMK2b 3DES CFB režiimis, kus ICV="00 00 00 00 00 00 00 00". Tulemus on:

MAC = **69 CA B6 19 A6 EC 60 C9**

Kuna see tulemus on võrdne kaardilt saabunud MAC-koodiga, siis võib lugeda võtme edukalt genereerituks.

Järgnevalt tuleb kaardilt välja lugeda avalik võti, et kasutada seda näiteks sertifikaadipäringu moodustamiseks.

Märkus: Avalik võti tuleb kaardilt välja lugeda hiljemalt enne järgmist võtmegenereerimise operatsiooni, sest EstEID kaardil on ainult üks avaliku võtme fail (FID=EEEE\1000) ning järgmisel võtmegenereerimise operatsioonil kirjutatakse selle faili sisu üle.

24) Loeme kaardilt välja avaliku võtme. Avalik võti on failis FID=EEEE\1000. See on jadafail pikkusega on 0x12C baiti. Faili struktuur on järgmine:

Baidid	**Sisu**
0..0x19	Püsiväärtused
0x20..0x9F	**Moodul**
0xA0..0xA1	Püsiväärtused
0xA1	**Avaliku eksponendi pikkus, 0x3 või 0x4 baiti**
0xA2..0xA4 või 0xA2..0xA5	**Avalik eksponent**
0xA6..0xAB	Püsiväärtused
0xAC..0x12B	Autentimisvõtmega arvutatud võtme allkiri (RSA, SHA-1, PKCS#1)

Selle võtme seadmiseks jooksvaks võtmeks tuleb modifitseerida faili FID=EEEE\0033 kirjet nr 1 (ainsat kirjet selles failis). See võib toimuda näiteks pärast genereeritud võtme kohta väljastatud sertifikaadi laadimist kaardile.

Faili FID=EEEE\0033 kirje nr 1 modifitseerimine võib toimuda sel viisil, et kirje loetakse failist välja, asendatakse väljaloetud kirjesse genereeritud võtme viit ning seejärel kirjutatakse kirje sisu faili tagasi. See kirje on failist vabalt loetav, kuid ülekirjutamiseks on

vajalik Kaardihalduskeskuse autoriseering.

Autoriseeringu saamiseks toimime järgnevalt:

Olgu kirje uus sisu järgmine:

Püsiväärtused	Autentimisvõtme viit	Püsiväärtused	Signeerimisvõtme viit
00 A4 08 95 01 40 83 03 80	**12 00**	B6 08 95 01 40 83 03 80	**02 00**

Selline kirje sisu tekib näiteks siis, kui pärast kaardi personaliseerimist on genereeritud uus autentimisvõti ja uus signeerimisvõti.

25) Seame kaardisisese turvakeskkonna nr 3 nii juurkataloogis kui EEEE kataloogis:

Valime juurkataloogi:

CLA	INS	P1	P2
00	**A4**	**00**	**0C**

Seame kaardisisese turvakeskkonna nr 3:

CLA	INS	P1	P2
00	**22**	**F3**	**03**

Valime kataloogi EEEE:

CLA	INS	P1	P2	Lc	FID	
00	**A4**	**01**	**0C**	**02**	**EE**	**EE**

Seame **uuesti** kaardisisese turvakeskkonna nr 3:

CLA	INS	P1	P2
00	**22**	**F3**	**03**

26) Valime faili FID=0033.

27) Verifitseerime PIN1.

28) Moodustame järgmise käsu:

Päis	Lc	Kirje sisu	Le
00 DC 01 04	**15**	00 A4 08 95 01 40 83 03 80 12 00 B6 08 95 01 40 83 03 80 02 00	00

29) Modifitseerime kirje päist nii:

Päis
0C DC 01 04

30) Moodustame järgmise bloki:

Püsiväärtused	Kirje sisu
81 15	00 A4 08 95 01 40 83 03 80 12 00 B6 08 95 01 40 83 03 80 02 00

31) Moodustame ajutiselt järgmise bloki:

Päis	Päise laiendus pikkuseni 8	Eelmisel sammul moodustatud andmeblokk	Eelmisel sammul moodustatud andmebloki laiendus pikkuseni, mis on 8 kordne
0C DC 01 04	**80 00 00 00**	81 15 …02 00	**80**

32) Arvutame selle bloki MAC-koodi 3DES CBC režiimis **kaardikohase võtmega CMK2b**, kus ICV=”00 00 00 00 00 00 00 00”. Meie näites on tulemus:

MAC = **4C C0 4E A0 22 E6 2D 9F**

33) Moodustame järgmise käsu, mille saadame kaardile:

Päis	Lc	Sammul 30 moodustatud blokk	Püsiväärtused	Sammul 32 arvutatud MAC	Le
0C DC 01 04	21	81 15 … 02 00	8E 08	4C C0 4E A0 22 E6 2D 9F	00

Märkus: Analoogselt sammul 11 moodustatud käsuga on ka see käsk kasutatav korduvalt, kuna ei sisalda sessiooni-spetsiifilist elementi.

Kaart vastab:

Püsiväärtused	OK Trailer’	Püsiväärtused	MAC	OK Trailer
99 02	**90 00**	8E 08	F9 5D 3F 23 71 D5 B7 11	**90 00**

Kui OK Trailer ja OK Trailer’ on mõlemad “90 00”, siis on faili FID=EEEE\0033 kirje nr 1 sisu edukalt üle kirjutatud ning näidatud viitadega võtmed seatud jooksvateks võtmeteks.

17.4. Sertifikaatide laadimismoodulite genereerimine

Sertifikaadi laadimismoodul sisaldab APDU-käsujadasid, mis EstEID kaardile saadetuna laevad sellele uue sertifikaadi (vt ka peatükki 13 “Sertifikaatide uuendamine” juhendi esimeses osas). Faili struktuur on järgmine:

Rida 1: Käsk SELECT FILE, mis valib ülekirjutamiseks õige faili.
Read 2..N: Käsud UPDATE BINARY, mis kirjutavad valitud faili uue sertifikaadi.

Käsud on kodeeritud BCD HEX kujul.

UPDATE BINARY käsud ridadel 2..N tuleb turvata, kasutades kaardikohast võtit CMK2b. Käsku SELECT FILE real 1 turvata ei tule.

Setifikaadifailide suurus EstEID kaardil on 0x600 baiti (seda võidakse edaspidi vastava vajaduse tekkimisel pädeva institutsiooni korraldusega suureneda). Failis pärast sertifikaadi kirjutamist vabaks jääv ruum tuleb täita järgmiselt:

0x600 baiti		
Sertifikaat	**Bait 0x80**	**Nullbaidid sertifikaadi lõpuni 00…00**

Turvatud UPDATE BINARY käskude lõppu tuleb lisada Le=0. Sertifikaati kaardile laadiv tarkvara, mis kasutab protokolli T=0, peab seda baiti ignoreerima.

Vaatame sertifikaadi laadimismooduli genereerimist järgmise näite varal. Olgu meil uus autentimissertifikaat (sertifikaat on näite selguse huvides lühendatud):

Baidid nr	Väärtused
0..F	30 82 04 A5 30 82 03 8D A0 03 02 01 02 02 04 3C
10..1F	02 31 6F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05
20..2F	05 00 30 68 31 0B 30 09 06 03 55 04 06 13 02 45
30..3F	45 31 22 30 20 06 03 55 04 0A 13 19 41 53 20 53
40..4F	65 72 74 69 66 69 74 73 65 65 72 69 6D 69 73 6B
50..5F	65 73 6B 75 73 31 10 30 0E 06 03 55 04 0B 13 07
60..6F	54 45 53 54 2D 53 4B 31 0A 30 08 06 03 55 04 04
70..7F	13 01 31 31 17 30 15 06 03 55 04 03 13 0E 54 45
80..8F	53 54 2D 45 53 54 45 49 44 2D 53 4B 30 1E 17 0D
90..9F	30 31 31 31 32 36 31 32 31 31 32 37 5A 17 0D 30
…..	….
400..40F	C0 88 E9 94 DB 6C DE FD 2A C8 5E 45 24 05 06 31
410..41F	04 25 69 D3 BF 74 38 7B 03 1C 12 D0 21 B6 A2 13
420..42F	58 5A 37 FE 1C B1 D9 3F 6E F7 E6 27 A1 EC B2 3C
430..43F	02 59 85 F3 36 7B 7B 14 A2 14 80 33 67 51 24 43
440..44F	B3 A2 55 8E F2 37 9C 6B 38 D0 EC 24 9D 37 5F 73
450..45F	99 E2 CE E0 5B 82 00 1B 69 4B AE 04 53 CA 39 EC
460..46F	42 1F 77 0E F1 44 10 C0 33 61 8D C3 B5 43 90 F7
470..47F	1E 6E EC EE 3F B3 8F C7 A9 CC 1F 07 B5 15 DD C8
480..48F	6F 4C C4 40 2A C0 A4 FF B7 2E 6D 98 FE 5A 06 D2
490..49F	DD 52 48 B9 F6 2A DE 9C DE 0C 8B 1F 84 44 5A D3
4A0..4A8	08 A8 AB 02 53 53 6D 80 5D

1) Moodustame faili kirjutatava andmebloki pikkusega 0x600 baiti:

Baidid nr	Väärtused
0..F	30 82 04 A5 30 82 03 8D A0 03 02 01 02 02 04 3C
10..1F	02 31 6F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05
20..2F	05 00 30 68 31 0B 30 09 06 03 55 04 06 13 02 45
30..3F	45 31 22 30 20 06 03 55 04 0A 13 19 41 53 20 53
40..4F	65 72 74 69 66 69 74 73 65 65 72 69 6D 69 73 6B
50..5F	65 73 6B 75 73 31 10 30 0E 06 03 55 04 0B 13 07
60..6F	54 45 53 54 2D 53 4B 31 0A 30 08 06 03 55 04 04
70..7F	13 01 31 31 17 30 15 06 03 55 04 03 13 0E 54 45
80..8F	53 54 2D 45 53 54 45 49 44 2D 53 4B 30 1E 17 0D
90..9F	30 31 31 31 32 36 31 32 31 31 32 37 5A 17 0D 30
…..	….
400..40F	C0 88 E9 94 DB 6C DE FD 2A C8 5E 45 24 05 06 31
410..41F	04 25 69 D3 BF 74 38 7B 03 1C 12 D0 21 B6 A2 13
420..42F	58 5A 37 FE 1C B1 D9 3F 6E F7 E6 27 A1 EC B2 3C
430..43F	02 59 85 F3 36 7B 7B 14 A2 14 80 33 67 51 24 43
440..44F	B3 A2 55 8E F2 37 9C 6B 38 D0 EC 24 9D 37 5F 73
450..45F	99 E2 CE E0 5B 82 00 1B 69 4B AE 04 53 CA 39 EC
460..46F	42 1F 77 0E F1 44 10 C0 33 61 8D C3 B5 43 90 F7
470..47F	1E 6E EC EE 3F B3 8F C7 A9 CC 1F 07 B5 15 DD C8
480..48F	6F 4C C4 40 2A C0 A4 FF B7 2E 6D 98 FE 5A 06 D2
490..49F	DD 52 48 B9 F6 2A DE 9C DE 0C 8B 1F 84 44 5A D3
4A0..4A8	08 A8 AB 02 53 53 6D 80 5D **80** 00 00 00 00 00 00
4B0..4BF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
…..	…..
590..59F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

2) Moodustame 1. rea – käsu SELECT FILE:

Päis	Lc	Sertifikaadi faili FID
00 A4 02 0C	**02**	**AA CE**

Signeerimissertifikaadi FID on **DDCE**.

Moodustame turvatud UPDATE BINARY käsud sertifikaadi kirjutamiseks kaardile. Soovitatav on ühe käsuga saata kaardile 0x40 või 0x40 kordne hulk baite (so. 0x80 või

0xC0), sest need väärtused on EstEID kiibi riistvara jaoks optimaalsed.

Alljärgnevalt vaatleme turvatud UPDATE BINARY käsu moodustamist sertifikaadi baitidest 0…0x40.

3) Moodustame käsu päise:

CLA	INS	P1 ofseti vanem bait	P2 ofseti noorem bait
0C	**D6**	**00**	**00**

4) Moodustame järgmise bloki

Püsiväärtus	Järgneva andmebloki pikkus	Sertifikaadi baidid 0..0x40
81	**40**	**30 82 04 A5 .. 41 53 20 53**

Märkus: Kui saadame ühe käsuga 0x80 või 0xC0 baiti, siis tuleb see andmeblokk moodustada järgmiselt (0x80 baidi korral):

Püsiväärtus	Püsiväärtus	Järgneva andmebloki pikkus	Sertifikaadi baidid 0..0x80
81	**81**	**80**	**30 82 04 A5 .. 03 55 04 04**

5) Moodustame ajutiselt järgmise bloki:

Päis	Päise laiendus pikkuseni 8	Eelmisel sammul moodustatud blokk	Eelmisel sammul moodustatud bloki laiendus pikkuseni, mis on 8 kordne
0C D6 00 00	**80 00 00 00**	**81 40 30 82 04 A5 … 41 53 20 53**	**80 00 00 00 00 00**

6) Arvutame selle bloki MAC-koodi 3DES CBC režiimis **kaardikohase võtmega CMK2b**, kus ICV=”00 00 00 00 00 00 00 00”. Tulemus on:

   MAC = **91 18 2F 52 15 BA 44 74**

7) Moodustame käsu järgmiselt:

Päis	Lc	Sammul 4 moodustatud blokk	Püsi-väärtused	Eelmisel sammul arvutatud MAC	Le
0C D6 00 00	**4C**	**81 40 30 82 04 A5 … 41 53 20 53**	**8E 08**	**91 18 2F 52 15 BA 44 74**	**00**

   NB! Käsu lõppu tuleb lisada bait Le=0. Sertifikaadi laadimise tarkvara, mis töötab protokolliga T=0, peab selle baidi enne käsu kaardile saatmist kõrvaldama.

Laadimiskoodi faili teine rida (esimene on käsk SELECT FILE) on seega valmis.

Samuti arvutame järgnevad read. Tulemus on:

Rida nr	Päis	Lc	Data	Le
1	00A4020C	02	AACE	
2	0CD60000	4C	8140308204A53082038DA00302010202043C02316F300D06092 A864886F70D01010505003068310B30090603550406130245453 1223020060355040A1319415320538E0891182F5215BA4474	00
3	0CD60040	4C	81406572746966697473656572696D69736B65736B7573311030 0E060355040B1307544553542D534B310A30080603550404130 131311730150603550403130E54458E08A0CA8956185B8EFC	00
4	0CD60080	4C	814053542D4553544549442D534B301E170D303131313236313 2313132375A170D30323034313431323534343 55A308191310B 300906035504061302656531 0F300D8E08716286E53AF42D1C	00
5	0CD600C	04	C8140060355040A13064553544549443117301506035504 0B130 E61757468656E7469636174696F6E3121301F060355040313184 5494B454547492C454556492C30308E0809AA438B73B3F7BC	00
6	0CD60100	4C	814030303030303030303031103 00E0603550404130745494B45 454749310D300B060355042A130445455649311430120603 5504 05130B30303030303030303030308E08318588C51D157F1F	00
7	0CD60140	4C	81403081A0300D06092A864886F70D01010105 0003818E00308 18A02818100BF588CF11BC7CA7D97A3D2F60CA8AF34212A76 A6BEDB0A2FB6BA4D6620347A605A0F7B8E0851A8E38B4BA8 9D6F	00
8	0CD60180	4C	81409761BB66846A6B82016F6558E580404D4DF4ECE49035D9 207ADE4C7A2497507D1AEF587CAE644705A7F6C145BF61C48 D7CA0E4943200EFFBB5096A8A86D71E7A8E084DDE851D9D4 FEECD	00
9	0CD601C0	4C	814052F615B815AE33E2E81D4C10CCF11A4ADD86867FA87A B5B5E41604397F02040231763FA38201AE308201AA300E0603 551D0F0101FF0404030204B0301D0603558E08ABDCB9BD898 95124	00
0xA	0CD60200	4C	81401D2504163014 06082B0601050507030206082B0601050507 030430380603551D1F0431302F302DA02BA0298627687474703 A2F2F7777772E736B2E65652F74658E08ADF4F99806354632	00
0xB	0CD60240	4C	8140737463726C2F6573746569642F63726C2E63726C300F060 3551D110408300681046E6F6E653082012C0603551D20048201 233082011F3082011B06092B0604018E080A4D5D4A7ECB547E	00
0xC	0CD60280	4C	8140CE1F0201023082010C3081E206082B06010505070202308 1D51E81D2005300650065002000730065007200740069006600 6 9006B00610061007400 20006F006E8E089CB18AF02C3142E2	00
	…	…	…	…
0x14	0CD60480	4C	81406F4CC4402AC0A4FFB72E6D98FE5A06D2DD5248B9F62A DE9CDE0C8B1F84445AD308A8AB0253536D805D800000000000 00000000000000000000000000000000008E08A68444C766072 48D	00
0x15	0CD604C0	4C	81400000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000 00000000000000000000000000008E08B31CB25697B76AC8	00
	…	…	…	…
0x19	0CD605C0	4C	81400000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000 00000000000000000000000000008E081105CEDAD9016710	00

17.5. PIN-koodide asendamine

PIN-koodide asendamine toimub järgmise kahe operatsiooni abil:

1. Kirjutatakse üle faili kirjed, kus hoitakse PIN-koodide väärtusi.
2. Initsialiseeritakse järjestikuste valesisestuste loendurid.

Vaatleme PIN-koodide asendamise protseduuri järgmise näite varal:

Olgu kaardi kasutaja isikukood “01234567890”, uus PIN1=”1234”, uus PIN2=”12345” ja uus PUK=”12345678”.

1) Järjestikuste valesisestuste loendurit saab initsialiseerida ainult siis, kui selle väärtus on 0 (kaart on blokeerunud). Seetõttu tuleb lugeda kaardilt järjestikuste valesisestuste loendurite väärtused (vt peatükk 8 “Loendurite lugemine kaardilt” juhendi I osas) ning kui need ei ole nullid, siis sooritada PIN-kontrolli operatsiooni vale PIN-koodiga, kuni nende loendurite väärtusteks saavad nullid.

2) Valime juurkataloogi:

CLA	INS	P1	P2
00	**A4**	**00**	**0C**

3) Valime FID=0012 (selles failis hoitakse PIN-koodide väärtusi)

CLA	INS	P1	P2	FID
00	**A4**	**02**	**0C**	**00 12**

4) Seame kaardisisese turvakeskkonna nr 4 juurkataloogis:

CLA	INS	P1	P2
00	**22**	**F3**	**04**

5) Järgnevalt tuletame sessioonivõtme analoogselt peatükis 3.3.2 punktides 3..9 tehtuga. 3DES võtmena kasutame kaardi **CMK1**, mille kaardisisene järjekorranumber on **1**.

Olgu meie juhul:

SK1 = 19 EB A2 29 ED EC 4F E9 E9 27 B4 FC 35 9E 8F DF
SK2 = 36 C3 42 23 9C B6 7F 0B EC 3B 04 8D C5 66 F2 30
SSC = 05 06 07 08 D2 86 CA 6F

6) PIN-koode ei hoita EstEID kaardil lahtisel kujul (vaatamata sellele, et nende faili FID=0012 lugemine on keelatud). Faili FID=0012 kirje on 9 baiti pikk ja selle struktuur on järgmine:

Bait nr.	0	1	2	3	4	5	6	7	8
Sisu	PIN-koodi pikkus	See blokk saadakse järgmiselt: 1. PIN-kood viiakse BCD HEX kujule ja lisatakse paremale väärtusi F pikkuseni 7 baiti. 2. Ette (vasakule) lisatakse bait väärtusega 0x20 + PIN-koodi pikkus 3. Krüptitakse see blokk DES algoritmiga, kasutades võtmena iseennast.							

Antud näites toimime PIN1-koodiga nii:

PIN blokk BCD HEX kujul:

Bait nr	0	1	2	3	4	5	6	7
Väätrus	**24**	**12**	**34**	**FF**	**FF**	**FF**	**FF**	**FF**

See blokk DES-krüptitult iseendaga: **7E B3 98 5F 23 22 9E 91**

Seega on PIN1 = “1234” kirje järgmine:

Bait nr.	0	1	2	3	4	5	6	7	8
Väärtus	04	**7E**	**B3**	**98**	**5F**	**23**	**22**	**9E**	**91**

PIN2 = “12345” blokk on: **05 1F 8A 25 12 DC EF 34 6C**.
PUK = “12345678” blokk on: **08 E6 76 6E 41 75 43 43 D5**.

Edasi vaatleme operatsiooni PIN1 näitel. PIN2- ja PUK-koodidega on operatsioon sarnane, erinevused on eraldi ära märgitud.

Järgnevalt sooritame operatsiooni UPDATE RECORD.

7) Moodustame käsu päise:

CLA	INS	P1 – PIN kirje number failis	P2 – püsiväärtus
0C	**DC**	**PIN1: 01** **PIN2: 02** **PUK: 03**	**04**

PIN1 korral:

CLA	INS	P1	P2
0C	**DC**	**01**	**04**

8) Suurendame sõnumiloendurit 1 võrra:

SSC = 05 06 07 08 D2 86 CA **70**

9) Moodustame järgmise bloki:

PIN-faili kirje	PIN-faili kirje laiendus pikkuseni, mis on 8 kordne
04 7E B3 98 5F 23 22 9E 91	**80 00 00 00 00 00 00**

10) Krüptime selle bloki võtmega SK1 3DES CBC režiimis, kus ICV=”00 00 00 00 00 00 00 00”. Tulemus on:

05 F0 E5 98 6D AD 9A 7E 92 02 27 EA B6 5A 75 5E

11) Moodustame järgmise bloki

Püsiväärtused	Eelmisel sammul saadud krüptoblokk
87 11 01	**05 F0 E5 98 6D AD 9A 7E 92 02 27 EA B6 5A 75 5E**

12) Moodustame ajutiselt järgmise bloki:

Päis	Päise laiendus pikkuseni 8	Eelmisel sammul moodustatud blokk	Eelmisel sammul moodustatud bloki laiendus pikkuseni, mis on 8 kordne
0C DC 01 04	**80 00 00 00**	**87 11 01 … 5A 75 5E**	**80 00 00 00 00**

13) Arvutame selle bloki MAC-koodi 3DES CFB režiimis võtmega **SK2**, kus ICV on sõnumiloendur. Tulemus on:

MAC = **AA 51 BE C6 12 AE 73 32**

14) Moodustame käsu, mille saadame kaardile (kui protokoll on T=0, ei ole Le vaja saaata):

Päis	Lc	Sammul 11 moodustatud blokk	Püsiväärtused	Eelmisel sammul saadud MAC	Le
0C DC 01 04	**1D**	**87 11 01 … 5A 75 5E**	**8E 08**	**AA 51 BE C6 12 AE 73 32**	**00**

Kaart vastab:

Püsiväärtused	OK Trailer'	Püsiväärtused	MAC	OK Trailer
99 02	**90 00**	**8E 08**	**EC 51 2D D9 B1 23 65 16**	**90 00**

Järgnevalt kontrollime kaardilt tulnud vastust.

15) Suurendame sõnumiloendurit 1 võrra:

SSC = 05 06 07 08 D2 86 CA **71**

16) Moodustame ajutiselt järgmise bloki:

Kaardilt tulnud vastus	Kaardilt tulnud vastuse laiendus pikkuseni 8
99 02 90 00	**80 00 00 00**

17) Arvutame selle bloki MAC-koodi 3DES CFB režiimis võtmega **SK2**, kus ICV on sõnumiloendur. Tulemus on:

MAC = **EC 51 2D D9 B1 23 65 16**

Kuna kaardilt saabunud MAC-kood võrdub arvutatud MAC-koodiga, siis võime lugeda faili FID=0012 (PIN-koodide fail) kirje edukalt ülekirjutatuks.

Järgnevalt tuleb veel taastada PIN-koodi järjestikuste valesisestuste loenduri väärtus. Seda teeme käsuga RESET RETRY COUNTER.

18) Moodustame käsu päise:

CLA	INS	P1 – püsiväärtus	P2 – PIN järjekorranumber kaardis
0C	**2C**	**03**	**PIN1: 01** **PIN2: 02** **PUK: 00**

PIN1 korral:

CLA	INS	P1	P2
0C	**2C**	**03**	**01**

19) Suurendame sõnumiloendurit 1 võrra:

SSC = 05 06 07 08 D2 86 CA **72**

20) Moodustame ajutiselt järgmise bloki:

Päis	Päise laiendus pikkuseni 8
0C 2C 03 01	**80 00 00 00**

21) Arvutame selle bloki MAC-koodi 3DES CFB režiimis võtmega **SK2**, kus ICV on sõnumiloendur. Meie näites on tulemus:

MAC = **45 F6 E8 BB 84 DE C8 35**

22) Moodustame käsu, mille saadame kaardile (kui protokoll on T=0, ei ole Le vaja saata):

Päis	Lc	Püsiväärtused	Eelmisel sammul saadud MAC	Le
0C 2C 03 01	**0A**	**8E 08**	**45 F6 E8 BB 84 DE C8 35**	**00**

Kaart vastab:

Püsiväärtused	OK Trailer'	Püsiväärtused	MAC	OK Trailer
99 02	**90 00**	**8E 08**	**4A EC FC D6 EB 6D BF 0A**	**90 00**

Järgnevalt kontrollime kaardilt tulnud vastust.

23) Suurendame sõnumiloendurit 1 võrra:

SSC = 05 06 07 08 D2 86 CA **73**

24) Moodustame ajutiselt järgmise bloki:

Kaardilt tulnud vastus	Kaardilt tulnud vastuse laiendus pikkuseni 8
99 02 90 00	**80 00 00 00**

25) Arvutame selle bloki MAC-koodi 3DES CFB režiimis võtmega **SK2**, kus ICV on sõnumiloendur. Tulemus on:

MAC = **4A EC FC D6 EB 6D BF 0A**

Kuna kaardilt tulnud MAC-kood võrdub arvutatud MAC-koodiga, siis on järjestikuste valesisestuste loenduri algväärtus edukalt taastatud.

Kui soovime korraga asendada ka PIN2- ja PUK-koodid, tuleb korrata samme 7..25 neile vastavate väärtustega.

17.6. Lisarakenduste laadimismoodulite genereerimine

EstEID kaardile võib laadida lisarakendusi, kuid kaart võtab neid vastu vaid **kaardikohase CMK3** võtmega turvatult.

Vaatleme lisarakenduse laadimismooduli loomist näite varal. Järgmine APDU-käsk laeb kaardile rakenduse, milles on üks 0x100 baiti pikk fail. See fail on alati loetav, kuid faili kirjutamiseks on vaja, et oleks kontrollitud PIN1[10].

Päis	Lc	Data
00E03800	**77**	**62218201388302FFDD8410D233000001000001000000000000000018A010 5A1038B0101640062178205044100110283020030850200168A0105A103 8B01016400731E8302003085058001019000851180010190008001 02A407 950108830200016213820101830200 0A850201008A0105A1038B0102640 0**

Käsu turvamiseks toimime nii:

1) Moodustame järgmise bloki:

Püsiväärtus	Andmebloki pikkus	APDU-käsu andmeblokk
81	**77**	**62 21 82 … 02 64 00**

2) Modifitseerime käsu päist järgmiselt:

[10] Rakenduste programmeerimist selles juhendis ei käsitleta.

CLA	INS	P1	P2
0C	E0	38	00

3) Moodustame ajutiselt järgmise bloki:

Päis	Päise laiendus pikkuseni 8	Sammul 1 moodustatud blokk	Sammul 1 moodustatud bloki laiendus pikkuseni, mis on 8 kordne
0C E0 38 00	**80 00 00 00**	**81 77 62 … 02 64 00**	**80 00 00 00 00 00 00**

4) Arvutame selle bloki MAC-koodi 3DES CBC režiimis **kaardikohase võtmega CMK3,** kus ICV="00 00 00 00 00 00 00 00". Meie näites on tulemus:

MAC = **4B 5A F7 09 E8 53 10 1C**

5) Moodustame käsu järgmiselt:

Päis	Lc	Sammul 3moodustatud blokk	Püsi-väärtused	Eelmisel sammul arvutatud MAC	Le
0C E0 38 00	**83**	**81 77 62 … 02 64 00**	**8E 08**	**4B 5A F7 09 E8 53 10 1C**	**00**

NB! Käsu lõppu tuleb lisada bait Le=0. Lisarakenduse laadimise tarkvara, mis töötab protokolliga T=0, peab selle baidi enne käsu kaardile saatmist kõrvaldama.

Lisarakenduse laadimine on sarnane sertifikaadi laadimisega (vt peatükki 13 "Sertifikaatide uuendamine" juhendi I osas), kuid kataloogi EEEE ei ole vaja valida ning seada tuleb kaardisisene turvakeskkond nr 5.

18. EstEID kaardi sümmeetrilised krüptooperatsioonid

18.1. 3DES krüptimine CBC režiimis

3DES krüptimine CBC režiimis toimub järgnevalt (siin ICV on initsialisatsioonivektor ja 3DESKey on võti):

```
for ( i = 0 ;  i < BlokkideArv;  i++ )
{
        if ( i == 0 ) XOR(Blokk[0], ICV);
        else XOR( Blokk[i], Blokk[i-1]);
        3DESEncrypt ( Blokk[i], 3DESKey);
}
```

18.2. 3DES MAC CBC režiimis

3DES MAC-koodi arvutamine CBC režiimis toimub järgnevalt (siin 3DESKey on võti ja CalculaedMAC saab lõpptulemuse):

```
CalculatedMAC = Blokk[0];

for ( i = 0; i < NumBlocks; i++ )
{
        if ( i == (NumBlocks - 1) ) // Viimane blokk
        {
```

```
                    // 3DES ainult viimase blokiga
                    3DESEncrypt (CalculatedMAC, 3DESKey);
            }
            else
            {
                    // kõigi teiste blokkidega ühekordne DES
                    // 3DES võtme vasakpoolse osaga
                    DESEncrypt (3DESKey[K1], CalculatedMAC);
                    XOR ( CalculatedMAC, Blokk[i+1] );
            }
    }
```

18.3. 3DES MAC CFB režiimis

3DES MAC-koodi arvutamine CBC režiimis toimub järgnevalt (siin 3DESKey on võti, MACICV on initsialisatsioonivektor ja CalculaedMAC saab lõpptulemuse):

```
CalculatedMAC = MACICV;
DESEncrypt (CalculatedMAC, 3DESKey[K1]); // Ühekordne DES
                                                    // 3DES-võtme
                                                    // vasakpoolse osaga
XOR(CalculatedMAC, Blokk[0]);

for ( i = 0; i < NumBlocks; i++ )
{
        if ( i == (NumBlocks - 1) ) // Viimane blokk
        {
                // 3DES ainult viimase blokiga
                3DESEncrypt (CalculatedMAC, 3DESKey);
        }
        else
        {
                // kõigi teiste blokkidega ühekordne DES
                // 3DES võtme vasakpoolse osaga
                DESEncrypt (3DESKey[K1], CalculatedMAC);
                XOR ( CalculatedMAC, Blokk[i+1] );
        }
```

19. EstEID kaardi veateated

Veakood	Mnemoonika	Seletusi
62 81	CorruptDataWarning	Kontrollsumma on vale - viitab enamasti kaardi riknemisele
62 82	EndOfFileWarning EndOfRecordWarning	Le on liiga suur. Viitab katsele lugeda failist liiga palju baite korraga (maksimaalne on FE).
62 83	FileInvalidWarning	Valitav fail on deaktiveeritud (EstEID ei esine)

Veakood	Mnemoonika	Seletusi
64 00	CorruptDataError ExecutionError InconsistentDataError FileInvalidError UndefinedTechnicalProblemError	Viitab tõsisele andmete mittekonsistentsusele kas kaardirakenduses või kaardile saadetud käsus. Samuti võib see veateade tulla siis, kui proovitakse teha mitteettenähtud operatsiooni, näiteks kaardilt salajast võtit välja lugeda. Mittekonsistentsuse tekkepõhjuseks võib olla ka kaardi riknemine.
65 81	MemoryFailureError	EstEID kaardi EEPROM kirjutamine ebaõnnestus, kaart on riknenud.
67 00	TinyLeError	Le on liiga väike. See viga tekib ka siis, kui T=1 protokolli kasutades on Leära jäänud.
69 00	NoChvReferenceError NoKeyreferenceError	Kaardile saadetud käsk viitab PIN-koodile või võtmele, mida pole kaardil olemas.
69 81	IncompatibleFileStructureError	Kaardil olev failistruktuur ei võimalda saadetud käsku täita. N Näiteks - püütakse lisada kirjet faili, mis juba sisaldab maksimaalse lubatud kirjete arvu.
69 82	SecurityStatusNotSatisfiedError	Kaardile saadetud käsk nõuab, et eelnevalt oleks sooritatud kaardi kasutaja autoriseerimine. Näiteks PIN kontroll, mida aga tehtud ei ole. See viga tekib ka siis, kui PIN-koodi kontrolliti, kuid PIN oli vale.
69 83	AuthenticationBlockedError	PIN lubatud järjestikuste valesisestuste arv on täis. PIN on blokeeritud.
69 84	ReferencedDataInvalidatedError	PIN-koodi või võtit vms ei saa enam kasutada.
69 85	CommandExecutionOrderError, ConditionOfUseNotSatisfiedError	Kaardile saadetud käsk nõuab sellise objekti (tavaliselt võtme) kasutamist, mida antud tingimustes ei ole lubatud kasutada. Tavaliselt tekib siis, kui on määratud vale turvakeskkond (ingl. security environment).

Veakood	Mnemoonika	Seletusi
69 86	CommandNotAllowedError	Kaardile saadetud käsk ei ole antud tingimustes lubatud.
69 87	SmDataObjectsMissingError	Kaardile saadetud käsus puuduvad mõned turvatud kommunikatsiooni (ingl. secure messaging) teostamiseks vajalikud andmed.
69 88	SmDataObjectsIncorrectError	Kaardile saadetud turvatud käsus sisalduvad andmed on valed. See viga võib antud juhendis toodud operatsioonide juures esineda sertifikaadi laadimisel, kui kas käsk on moodustatud valesti või püütakse sertifikaati laadida valesse kaarti.
69 89	SmWithoutSessionkeysError	Puuduvad turvalise kommunikatsiooni jaoks vajalikud sessioonivõtmed.
6A80	IncorrectParametersDatafieldError	Vigased andmed käsus.
6A82	FileNotFoundError	Faili ei leitud
6A83	RecordNotFoundError	Kirjet ei leitud.
6A84	NotEnoughMemorySpaceError	Kaardi mälu on otsas (ei tohiks siin juhendis toodud operatsioonide piires esineda).
6A86	IncorrectParameterError	Valed parameetrid käsus.
6A87	LcInconsistentWithP1P2Error	Selline Lc ei ole selles käsus võimalik.
6A88	ReferencedDataNotFoundError	Viidatud andmed puuduvad.
6A89	FileExistError	Fail on juba olemas.
6A8A	DfNameExistError	Kataloog on juba olemas.
6B00	WrongParametersError	Valed parameetrid käsus.
6D00	InstructionCodeNotSupportedError	Saadetud käsus antud instruktsioonibaiti (INS) kaart ei tunne.
6E00	ClassNotSupportedError	Saadetud käsus antud klassibaiti (INS) kaart ei tunne.
6F00	NoPreciseDiagnosisError	Viitab sellele, et kaart ei sobi kokku antud lugeja või liidesega.